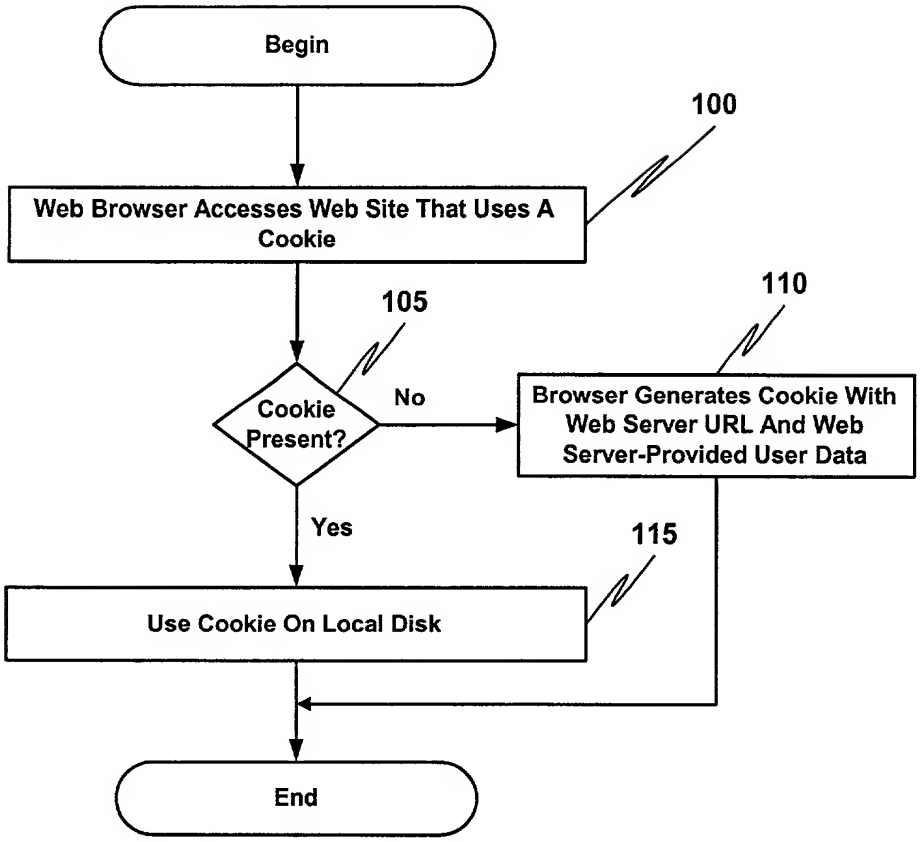


FIG. 1A

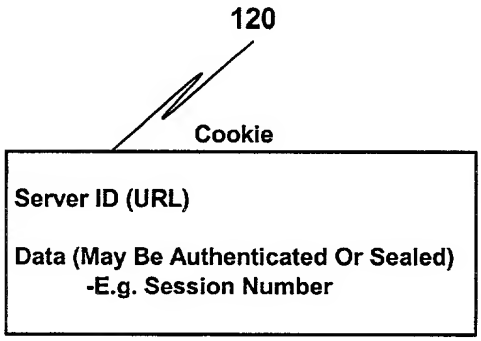


FIG. 1B - Prior Art

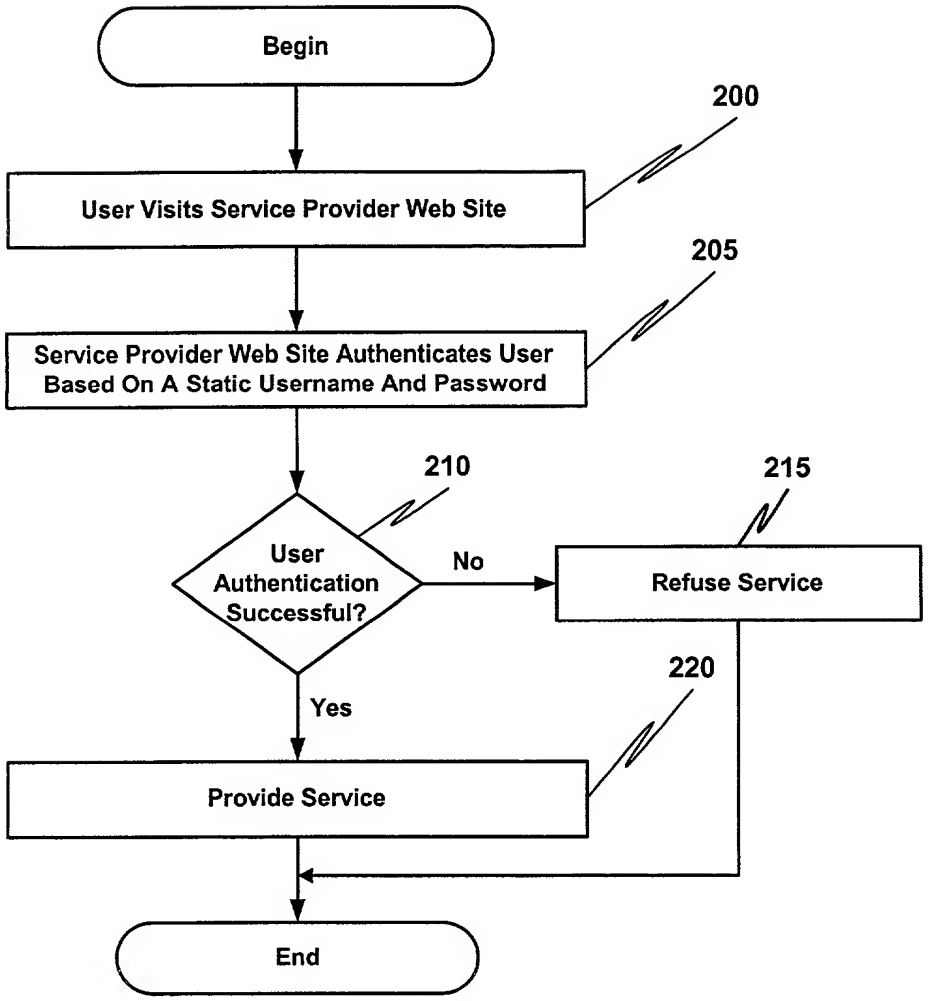


FIG. 2 - Prior Art

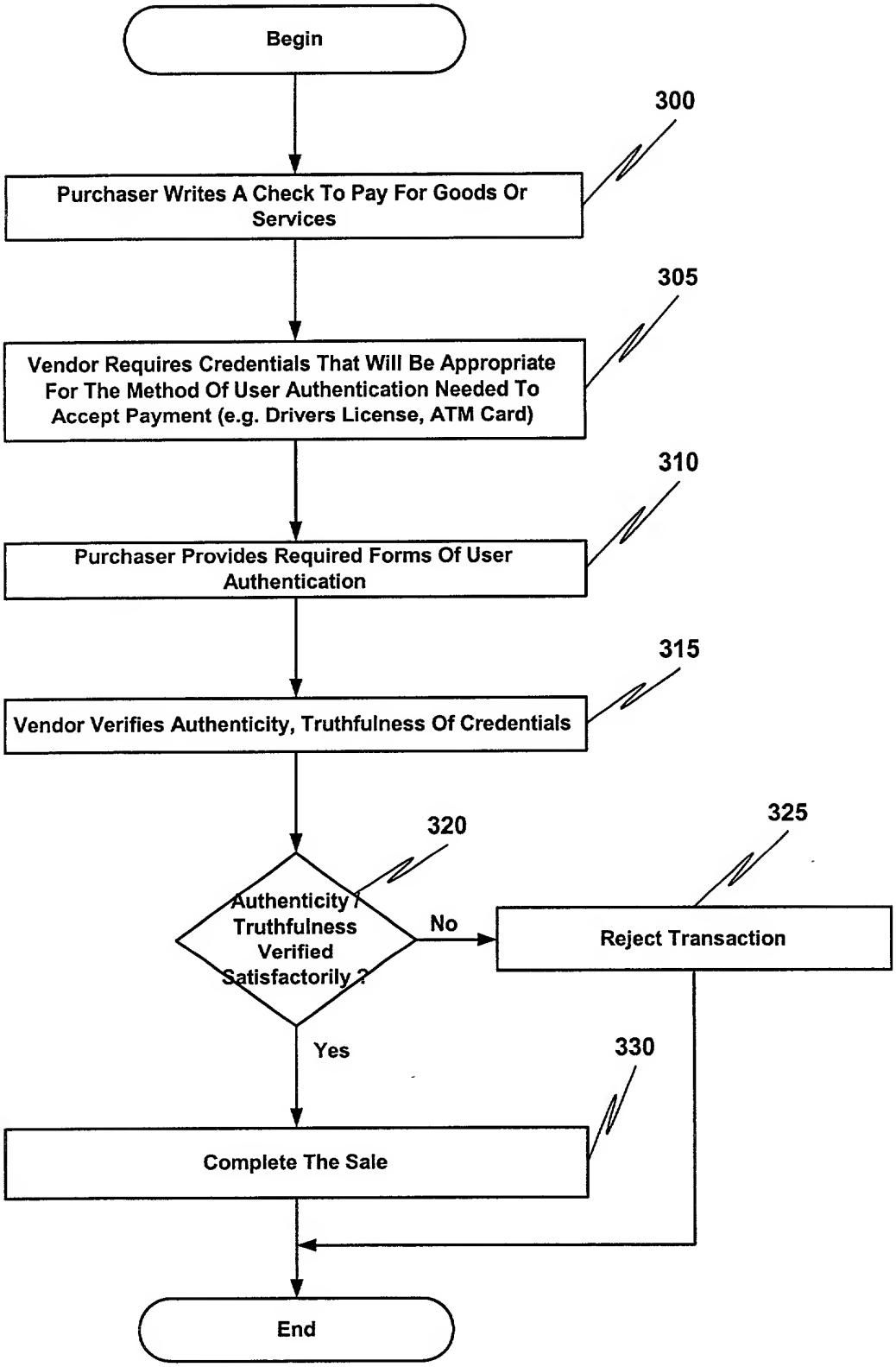


FIG. 3 - Prior Art

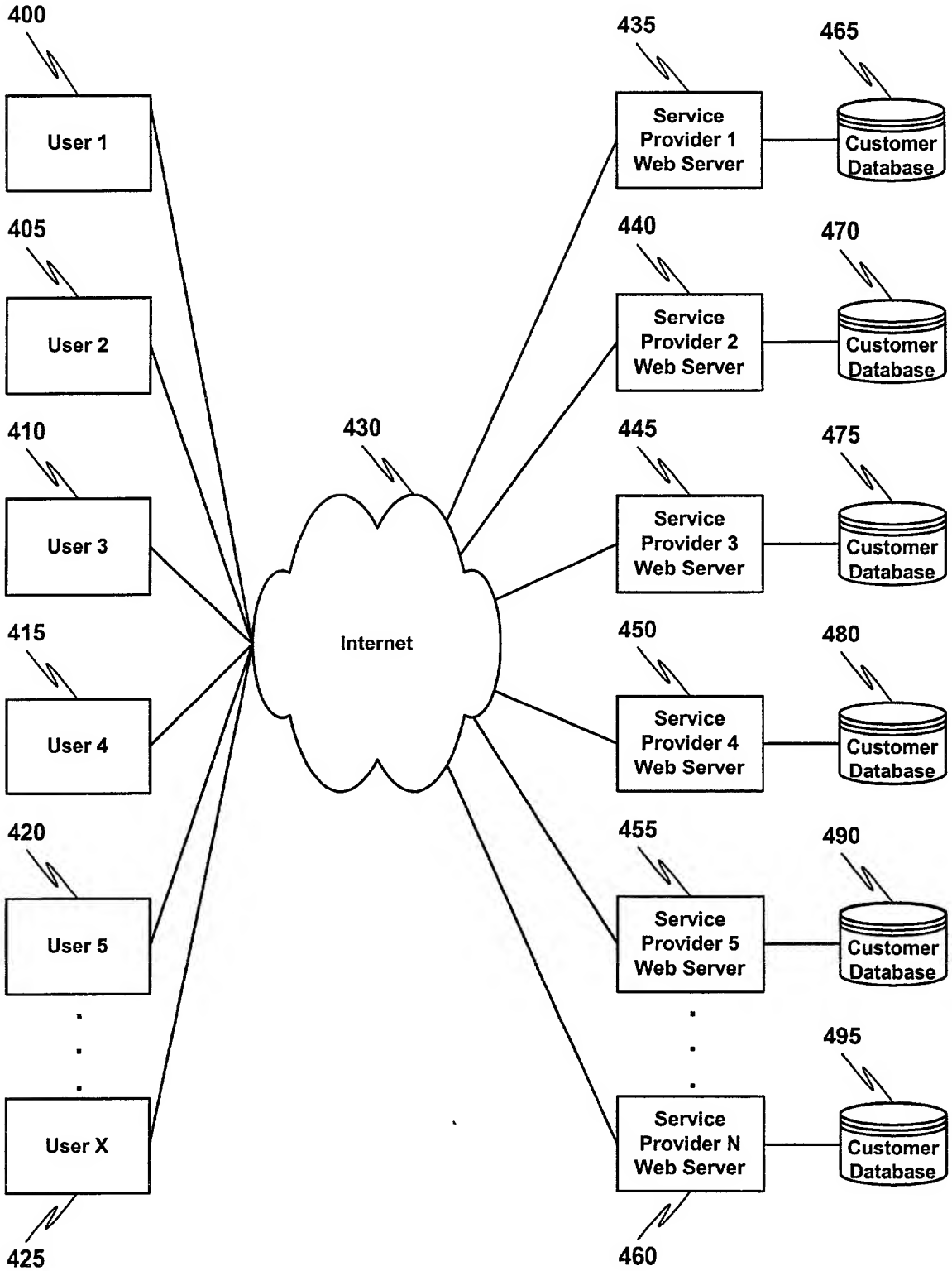


FIG. 4 - Prior Art

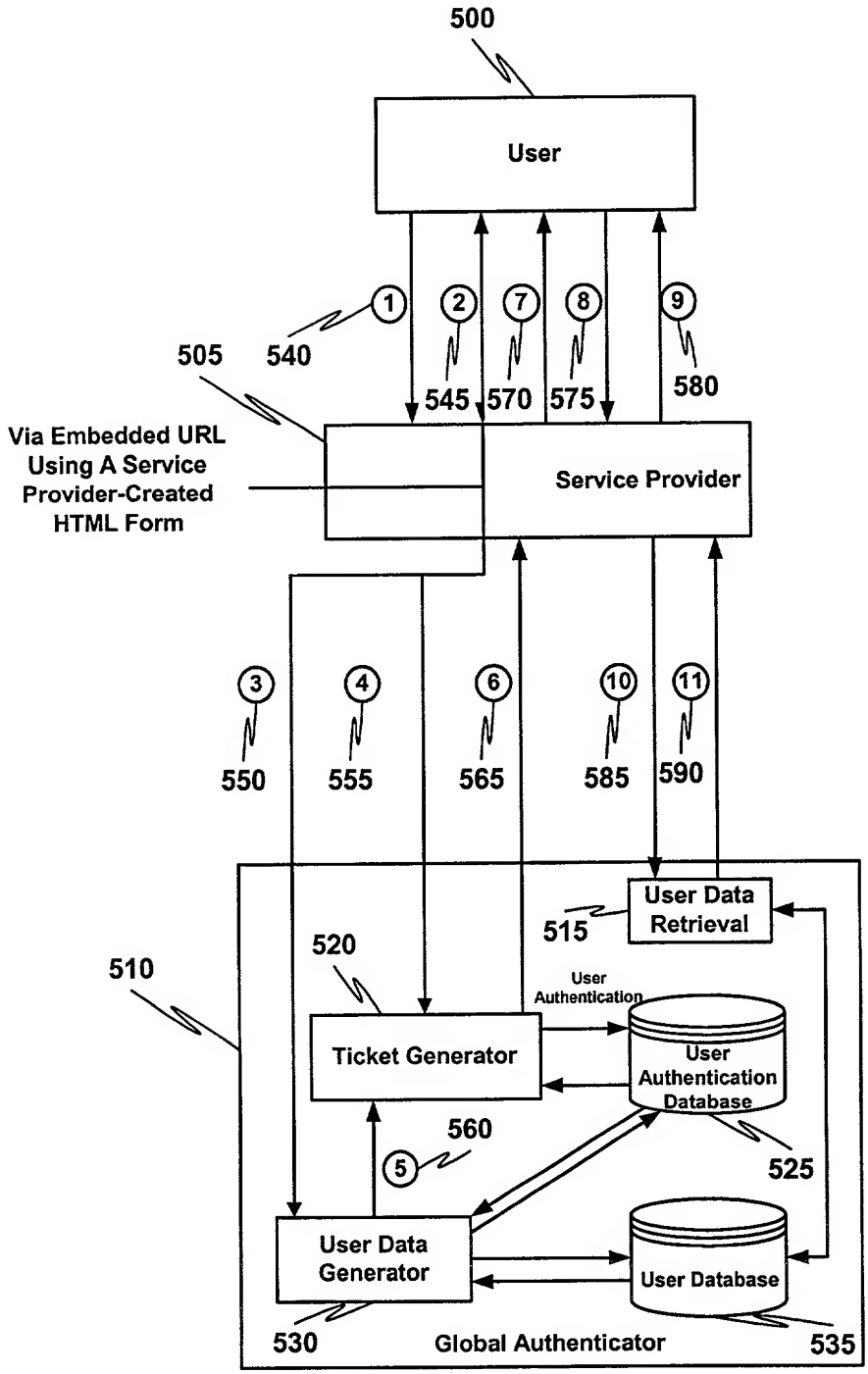


FIG. 5 - Prior Art

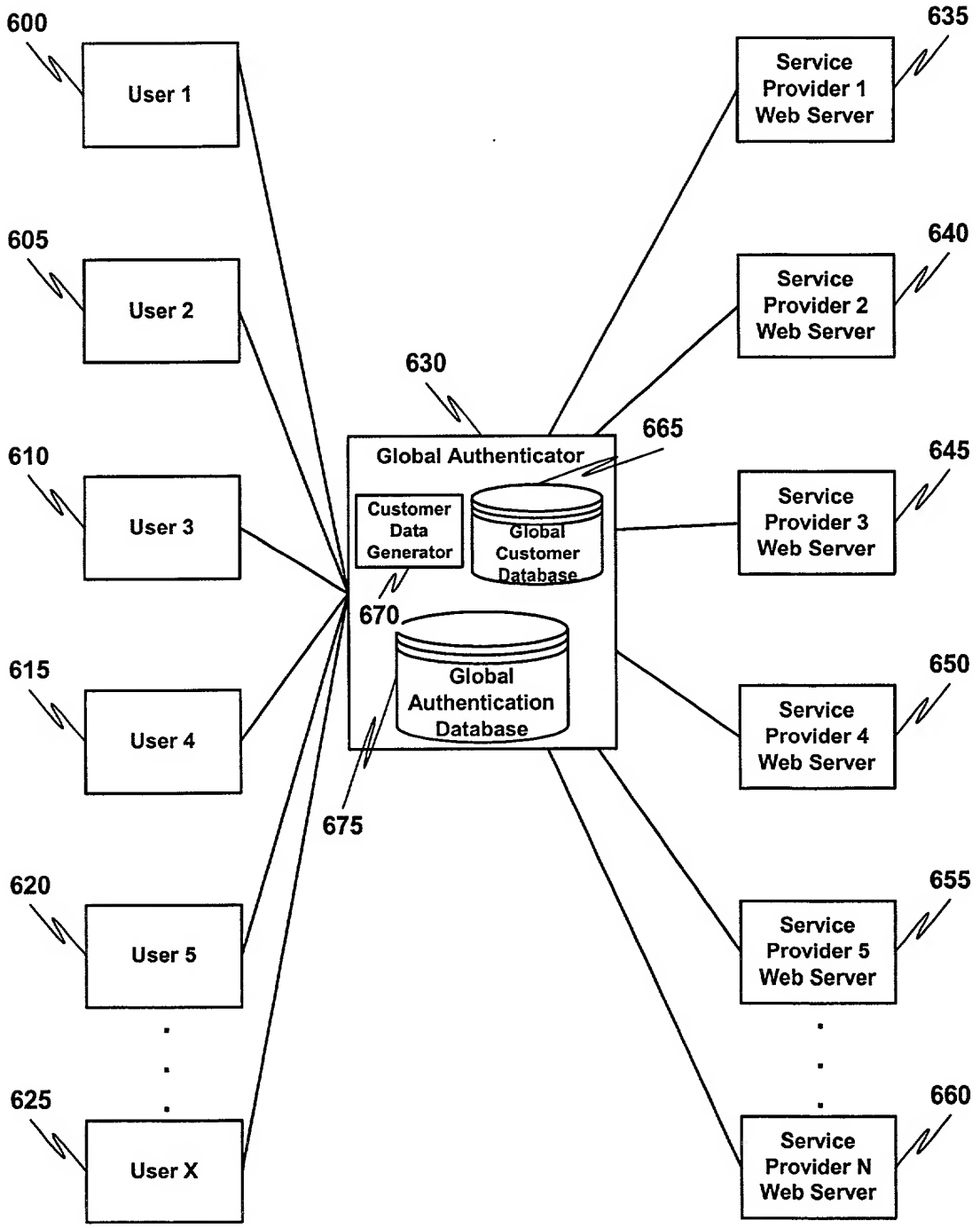


FIG. 6 - Prior Art

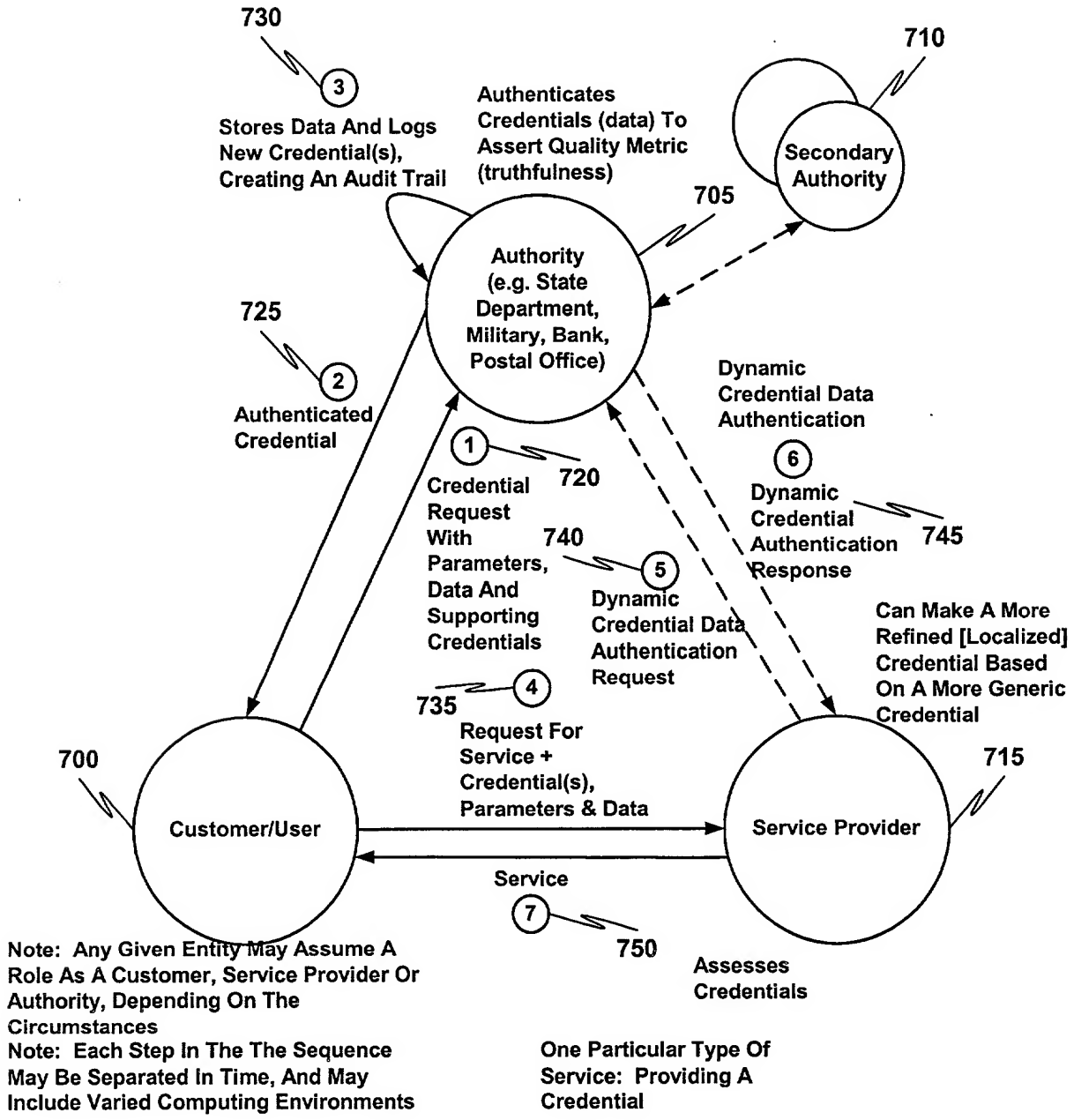
730
3
Stores Data And Logs New Credential(s), Creating An Audit Trail
Authenticates Credentials (data) To Assert Quality Metric (truthfulness)
710
Secondary Authority
705
Authority (e.g. State Department, Military, Bank, Postal Office)
725
2
Authenticated Credential
1
720
Credential Request With Parameters, Data And Supporting Credentials
740
5
Dynamic Credential Data Authentication Request
Dynamic Credential Data Authentication
6
Dynamic Credential Authentication Response
745
Can Make A More Refined [Localized] Credential Based On A More Generic Credential
735
4
Request For Service + Credential(s), Parameters & Data
700
Customer/User
715
Service Provider
Service
7
750
Assesses Credentials
Note: Any Given Entity May Assume A Role As A Customer, Service Provider Or Authority, Depending On The Circumstances
Note: Each Step In The The Sequence May Be Separated In Time, And May Include Varied Computing Environments
One Particular Type Of Service: Providing A Credential

FIG. 7

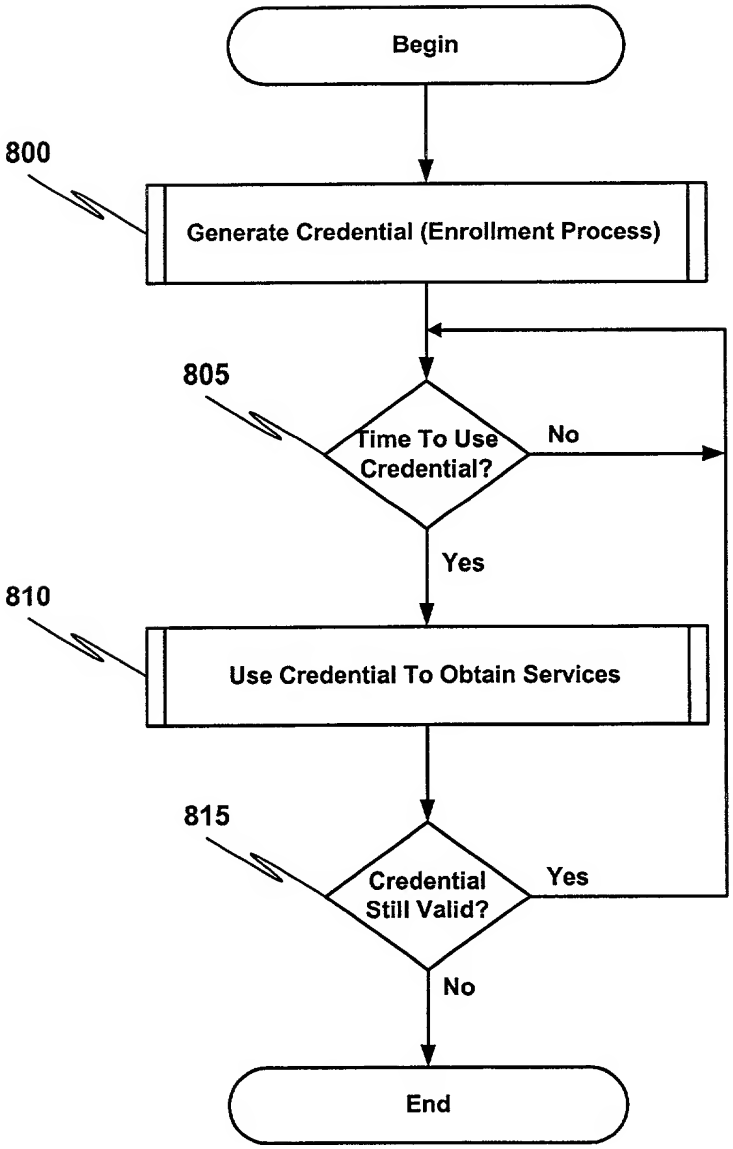
Begin
800
Generate Credential (Enrollment Process)
805
Time To Use Credential?
No
Yes
810
Use Credential To Obtain Services
815
Credential Still Valid?
Yes
No
End

FIG. 8

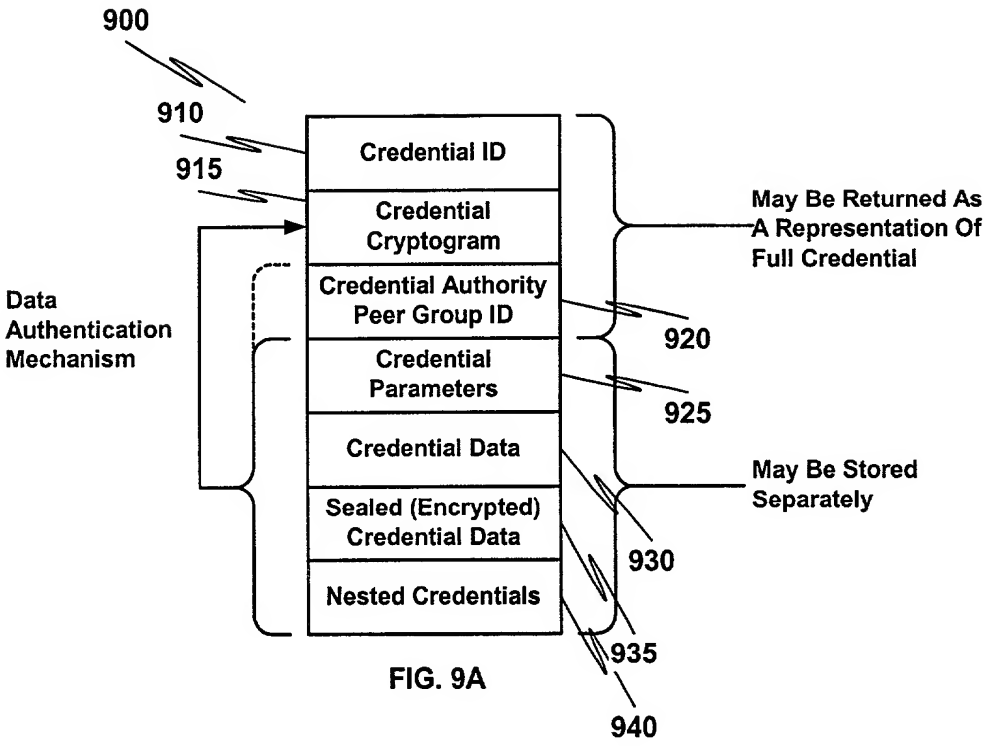
900
910
915
Credential ID
Credential Cryptogram
Credential Authority Peer Group ID
Credential Parameters
Credential Data
Sealed (Encrypted) Credential Data
Nested Credentials
Data Authentication Mechanism
May Be Returned As A Representation Of Full Credential
920
925
May Be Stored Separately
930
935
940

FIG. 9A

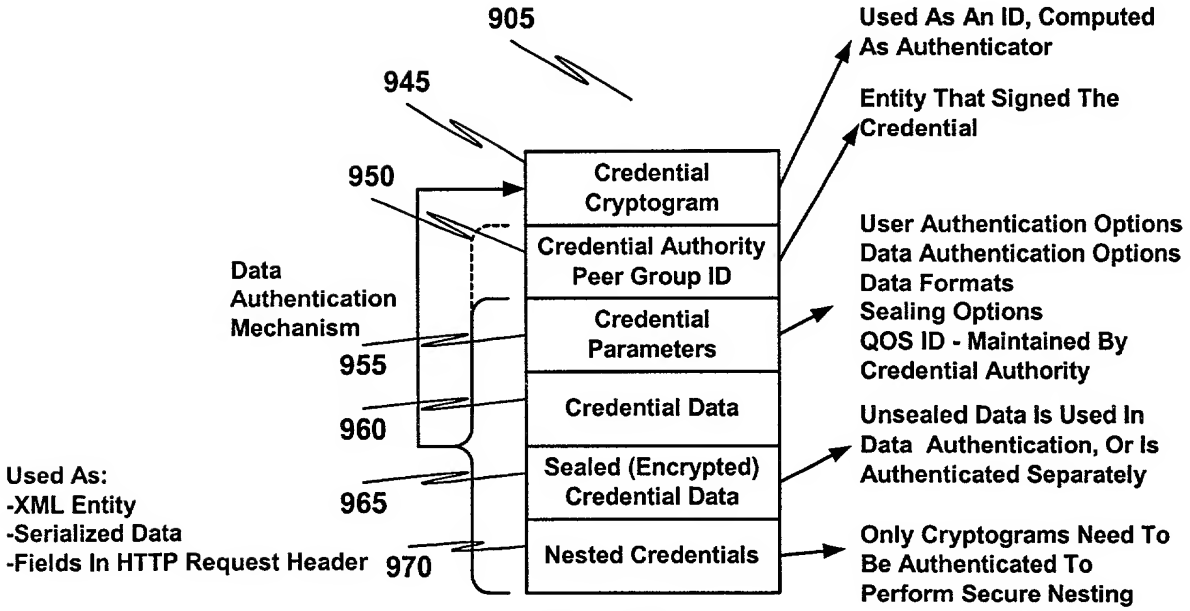
905
945
950
Credential Cryptogram
Credential Authority Peer Group ID
Credential Parameters
Credential Data
Sealed (Encrypted) Credential Data
Nested Credentials
Data Authentication Mechanism
955
960
965
970
Used As:
-XML Entity
-Serialized Data
-Fields In HTTP Request Header
Used As An ID, Computed As Authenticator
Entity That Signed The Credential
User Authentication Options
Data Authentication Options
Data Formats
Sealing Options
QOS ID - Maintained By Credential Authority
Unsealed Data Is Used In Data Authentication, Or Is Authenticated Separately
Only Cryptograms Need To Be Authenticated To Perform Secure Nesting

FIG. 9B

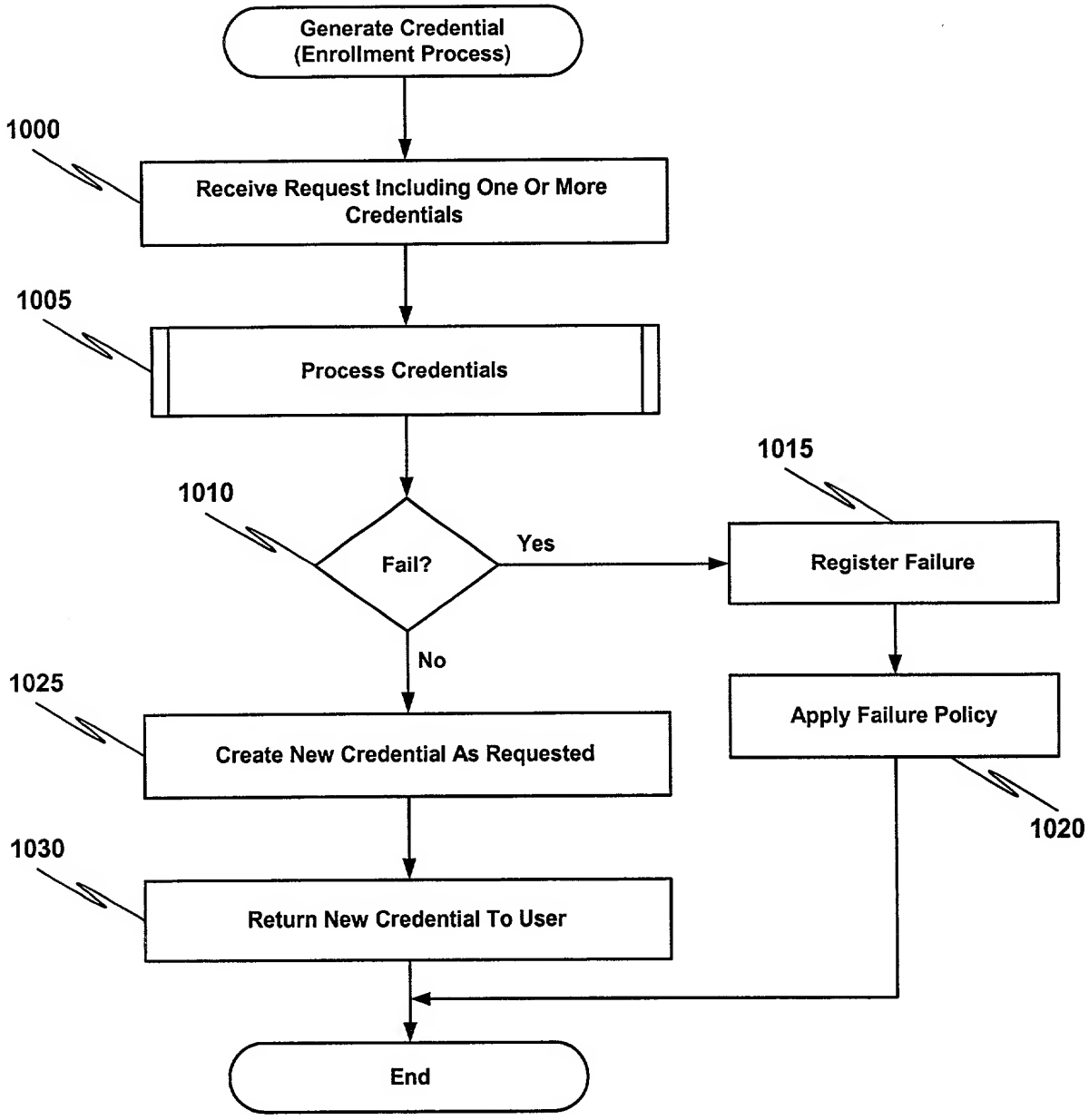
Generate Credential
(Enrollment Process)
1000
Receive Request Including One Or More Credentials
1005
Process Credentials
1010
Fail?
Yes
1015
Register Failure
No
1025
Create New Credential As Requested
Apply Failure Policy
1020
1030
Return New Credential To User
End

FIG. 10

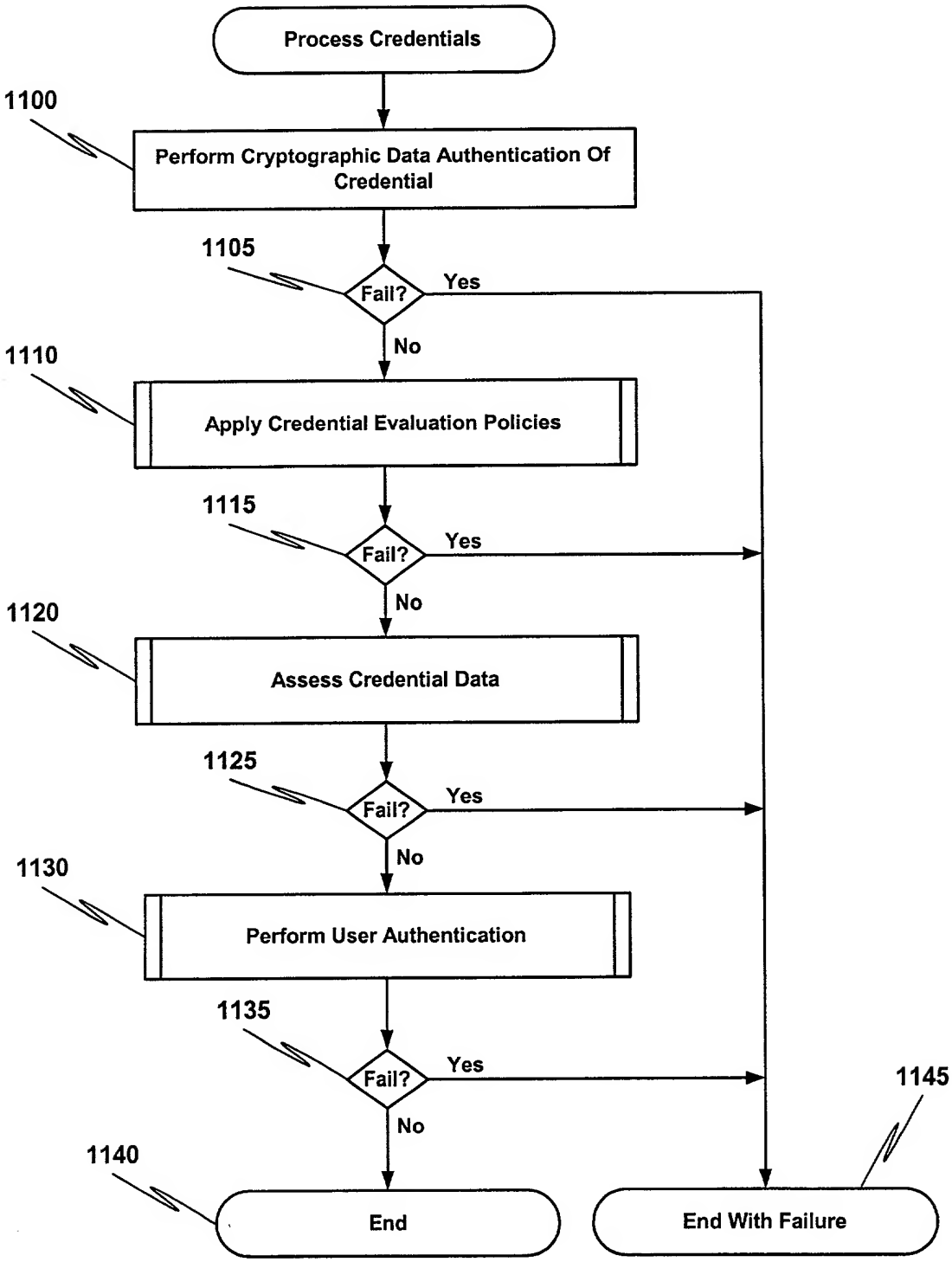
Process Credentials
1100
Perform Cryptographic Data Authentication Of Credential
1105
Fail?
Yes
No
1110
Apply Credential Evaluation Policies
1115
Fail?
Yes
No
1120
Assess Credential Data
1125
Fail?
Yes
No
1130
Perform User Authentication
1135
Fail?
Yes
No
1140
End
1145
End With Failure

FIG. 11

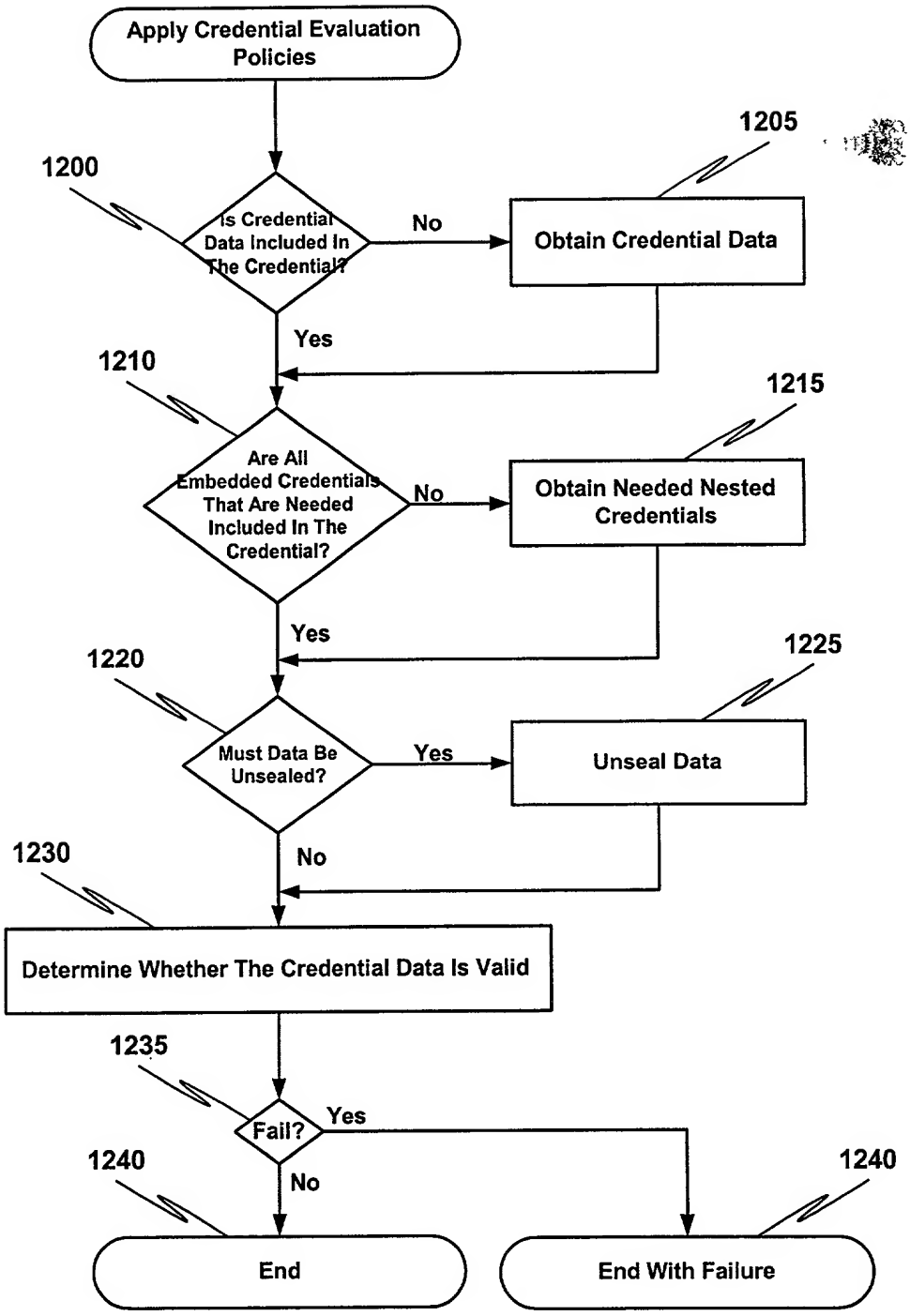
Apply Credential Evaluation Policies
1205
1200
Is Credential Data Included In The Credential?
No
Obtain Credential Data
Yes
1210
1215
Are All Embedded Credentials That Are Needed Included In The Credential?
No
Obtain Needed Nested Credentials
Yes
1220
1225
Must Data Be Unsealed?
Yes
Unseal Data
1230
No
Determine Whether The Credential Data Is Valid
1235
Fail?
Yes
1240
No
1240
End
End With Failure

FIG. 12

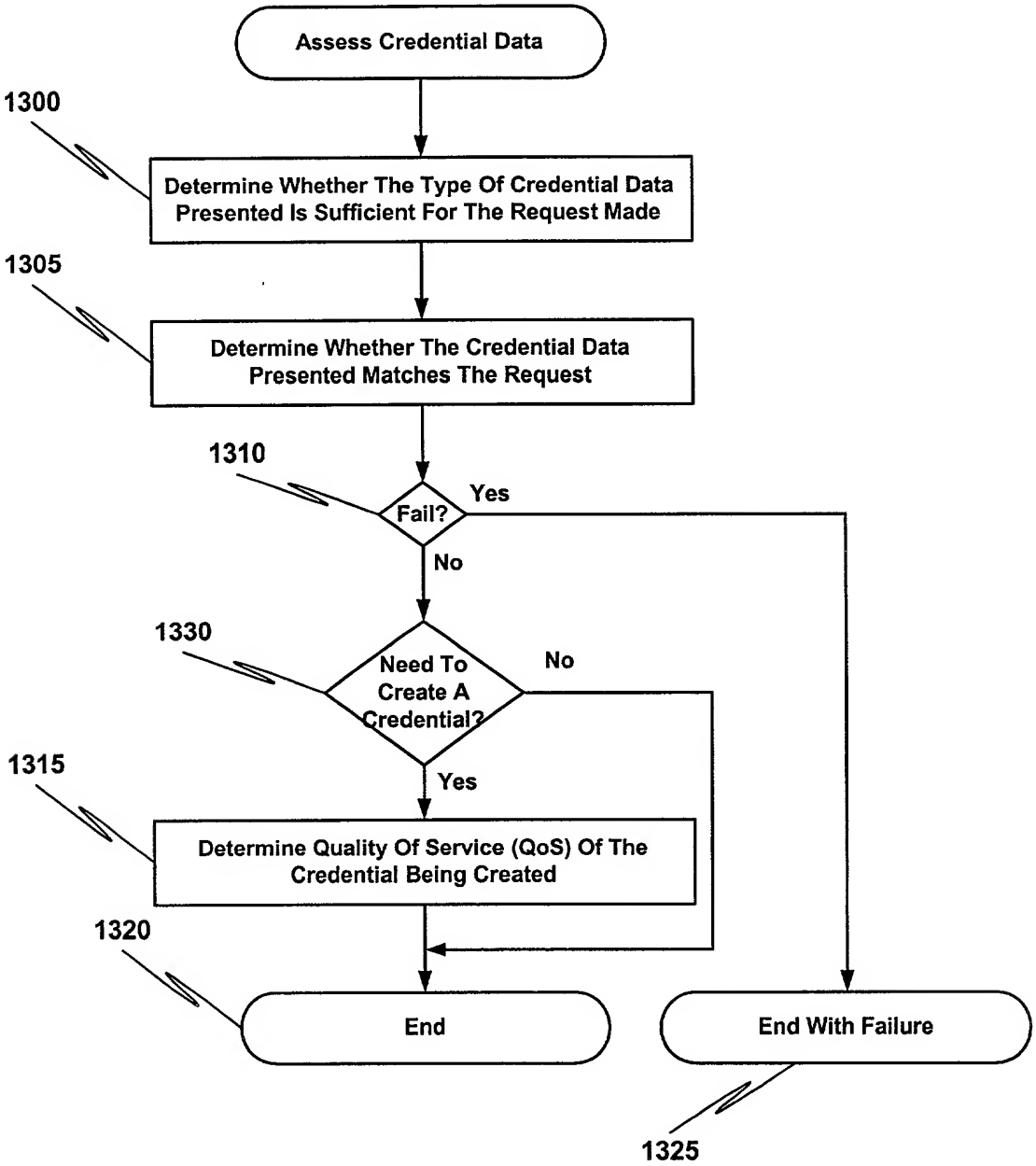
Assess Credential Data
1300
Determine Whether The Type Of Credential Data Presented Is Sufficient For The Request Made
1305
Determine Whether The Credential Data Presented Matches The Request
1310
Fail?
Yes
No
1330
Need To Create A Credential?
No
Yes
1315
Determine Quality Of Service (QoS) Of The Credential Being Created
1320
End
End With Failure
1325

FIG. 13

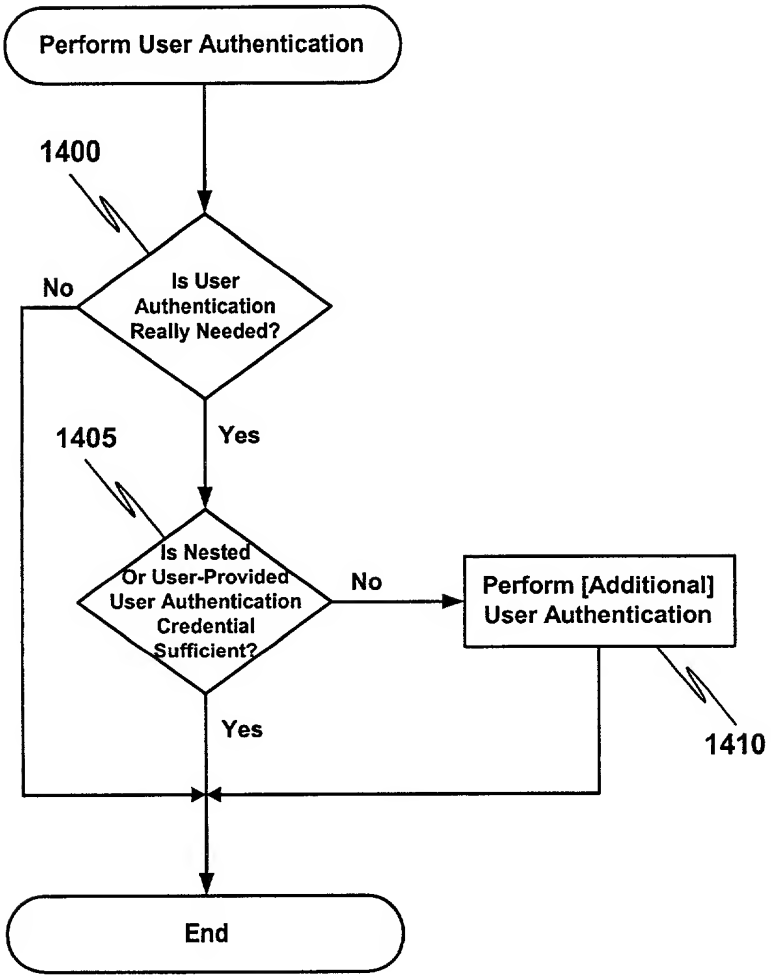
Perform User Authentication
1400
Is User Authentication Really Needed?
No
Yes
1405
Is Nested Or User-Provided User Authentication Credential Sufficient?
No
Perform [Additional] User Authentication
1410
Yes
End

FIG. 14

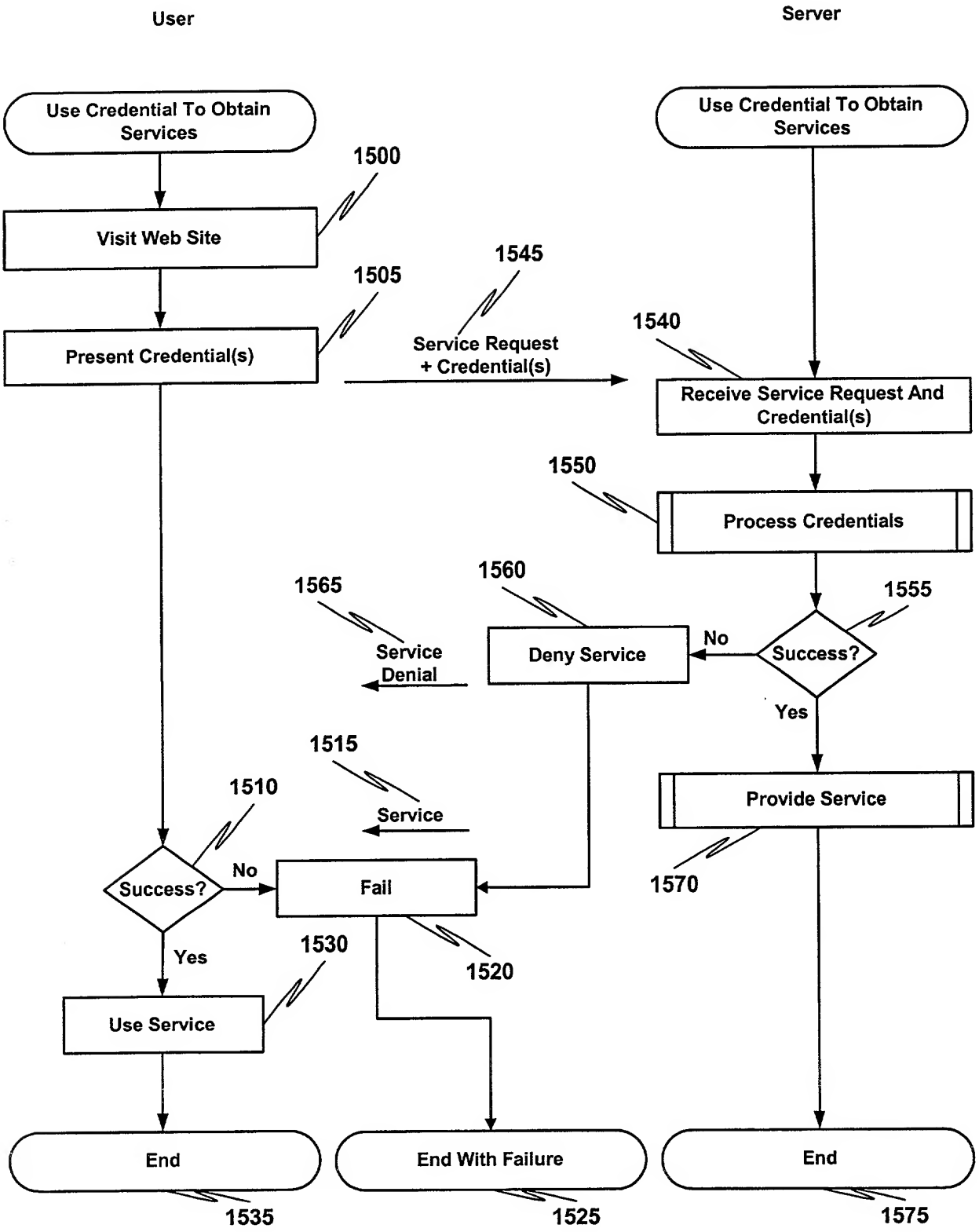
User
Server
Use Credential To Obtain Services
Use Credential To Obtain Services
1500
Visit Web Site
1545
1505
Present Credential(s)
Service Request + Credential(s)
1540
Receive Service Request And Credential(s)
1550
Process Credentials
1565
1560
1555
Service Denial
Deny Service
No
Success?
Yes
1515
Service
1510
Provide Service
Success?
No
Fail
1570
Yes
1530
1520
Use Service
End
End With Failure
End
1535
1525
1575

FIG. 15

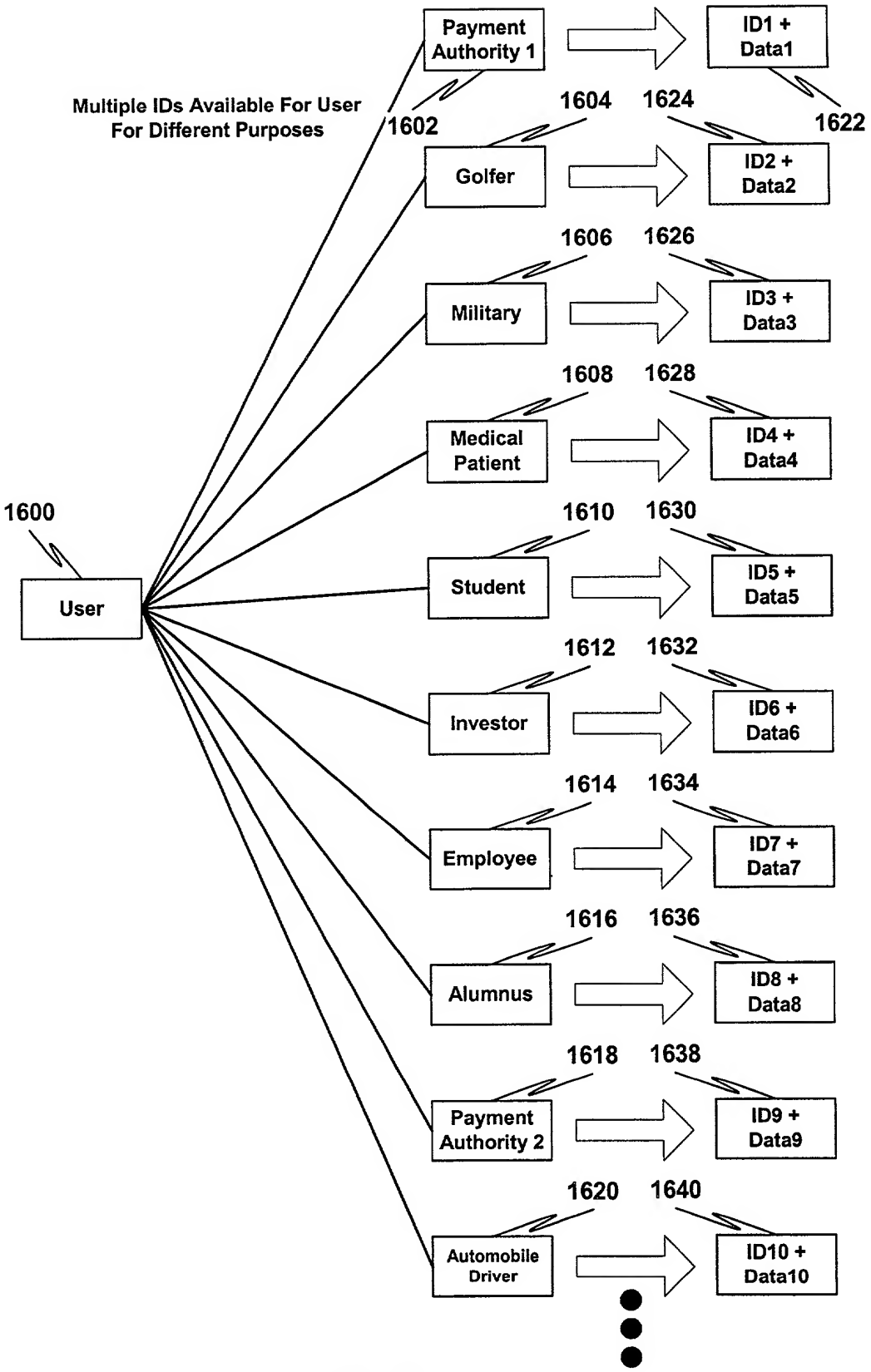
Multiple IDs Available For User For Different Purposes
1600
User
1602
Payment Authority 1
ID1 + Data1
1622
1604
1624
Golfer
ID2 + Data2
1606
1626
Military
ID3 + Data3
1608
1628
Medical Patient
ID4 + Data4
1610
1630
Student
ID5 + Data5
1612
1632
Investor
ID6 + Data6
1614
1634
Employee
ID7 + Data7
1616
1636
Alumnus
ID8 + Data8
1618
1638
Payment Authority 2
ID9 + Data9
1620
1640
Automobile Driver
ID10 + Data10

FIG. 16

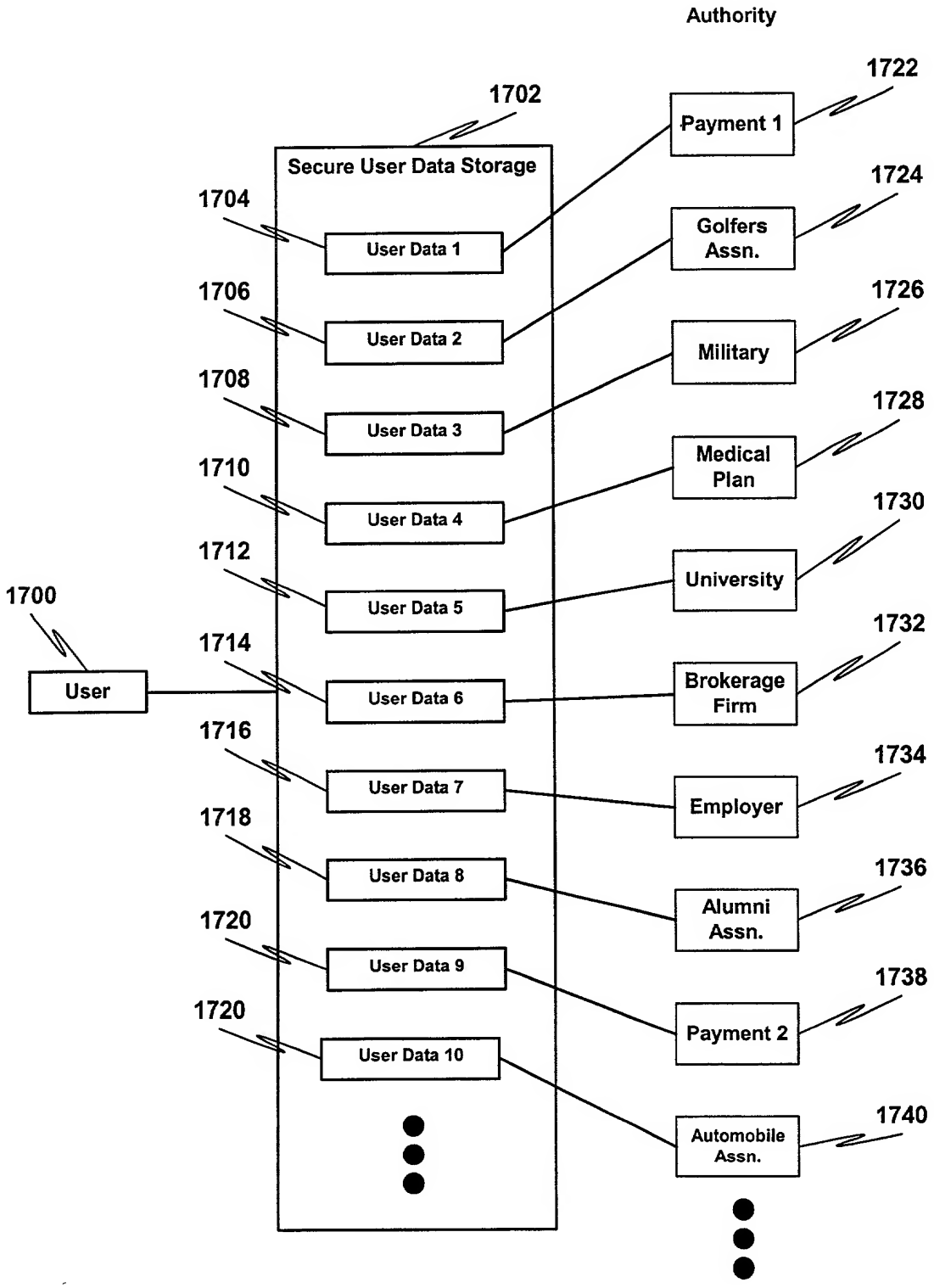
Authority
1722
1702
Payment 1
Secure User Data Storage
1724
1704
Golfers Assn.
User Data 1
1726
1706
Military
User Data 2
1728
1708
Medical Plan
User Data 3
1730
1710
University
User Data 4
1732
1712
Brokerage Firm
User Data 5
1700
1734
1714
Employer
User
User Data 6
1736
1716
Alumni Assn.
User Data 7
1738
1718
Payment 2
User Data 8
1740
1720
Automobile Assn.
User Data 9
1720
User Data 10

FIG. 17

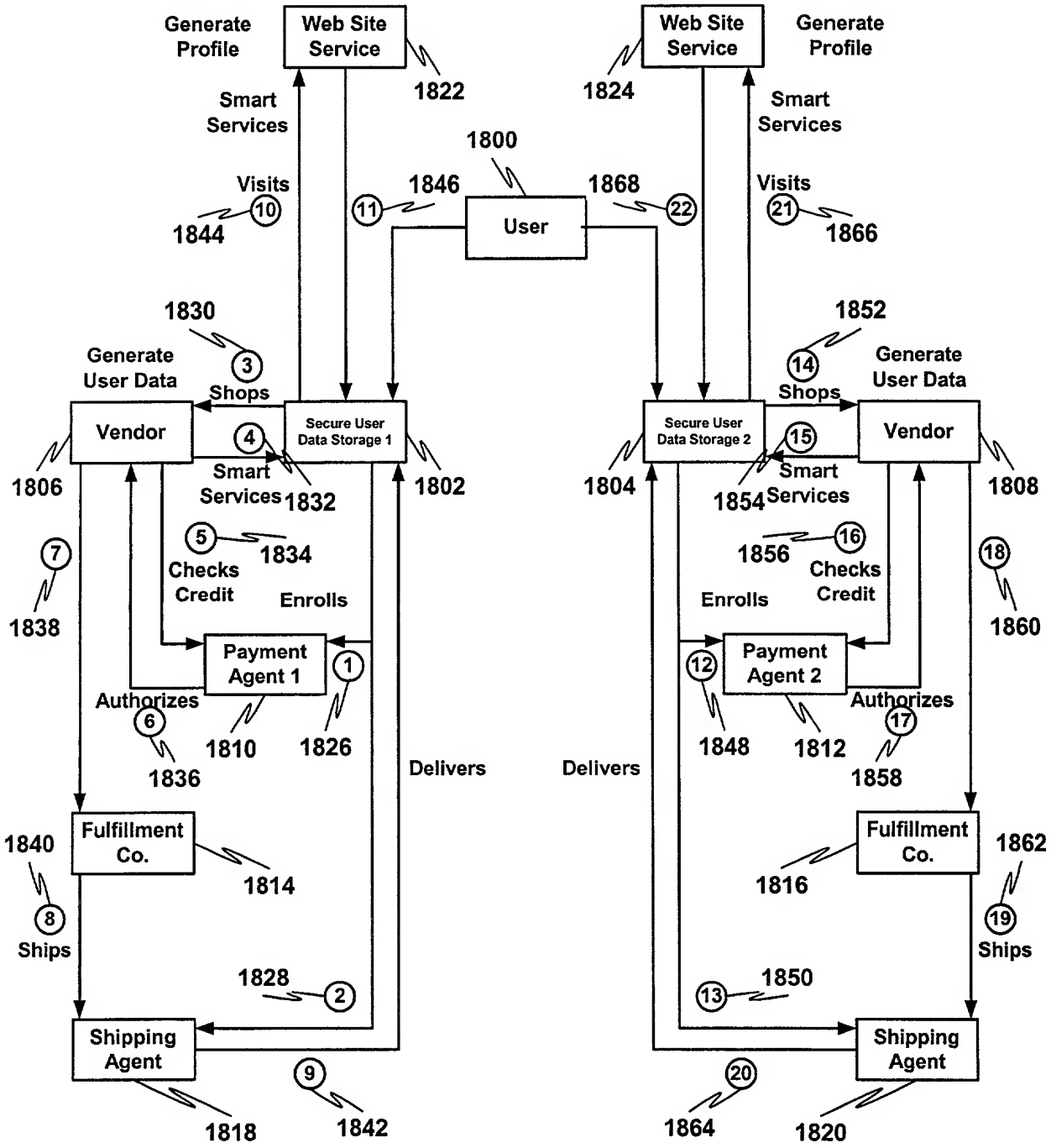
Generate Profile
Web Site Service
1822
1824
Web Site Service
Generate Profile
Smart Services
Smart Services
1800
Visits
1844
10
1846
11
User
1868
22
21
Visits
1866
1830
3
Generate User Data
Shops
Vendor
1806
4
Smart Services
1832
Secure User Data Storage 1
1802
1852
14
Generate User Data
Shops
Secure User Data Storage 2
15
Smart Services
1854
Vendor
1808
1804
5
1834
Checks Credit
Enrolls
7
1838
1856
16
Checks Credit
Enrolls
18
1860
Payment Agent 1
1
Authorizes
6
1836
1810
1826
Payment Agent 2
12
1848
1812
Authorizes
17
1858
Delivers
Delivers
Fulfillment Co.
1840
1814
8
Ships
Fulfillment Co.
1862
1816
19
Ships
1828
2
1850
13
Shipping Agent
9
1818
1842
Shipping Agent
20
1864
1820

FIG. 18

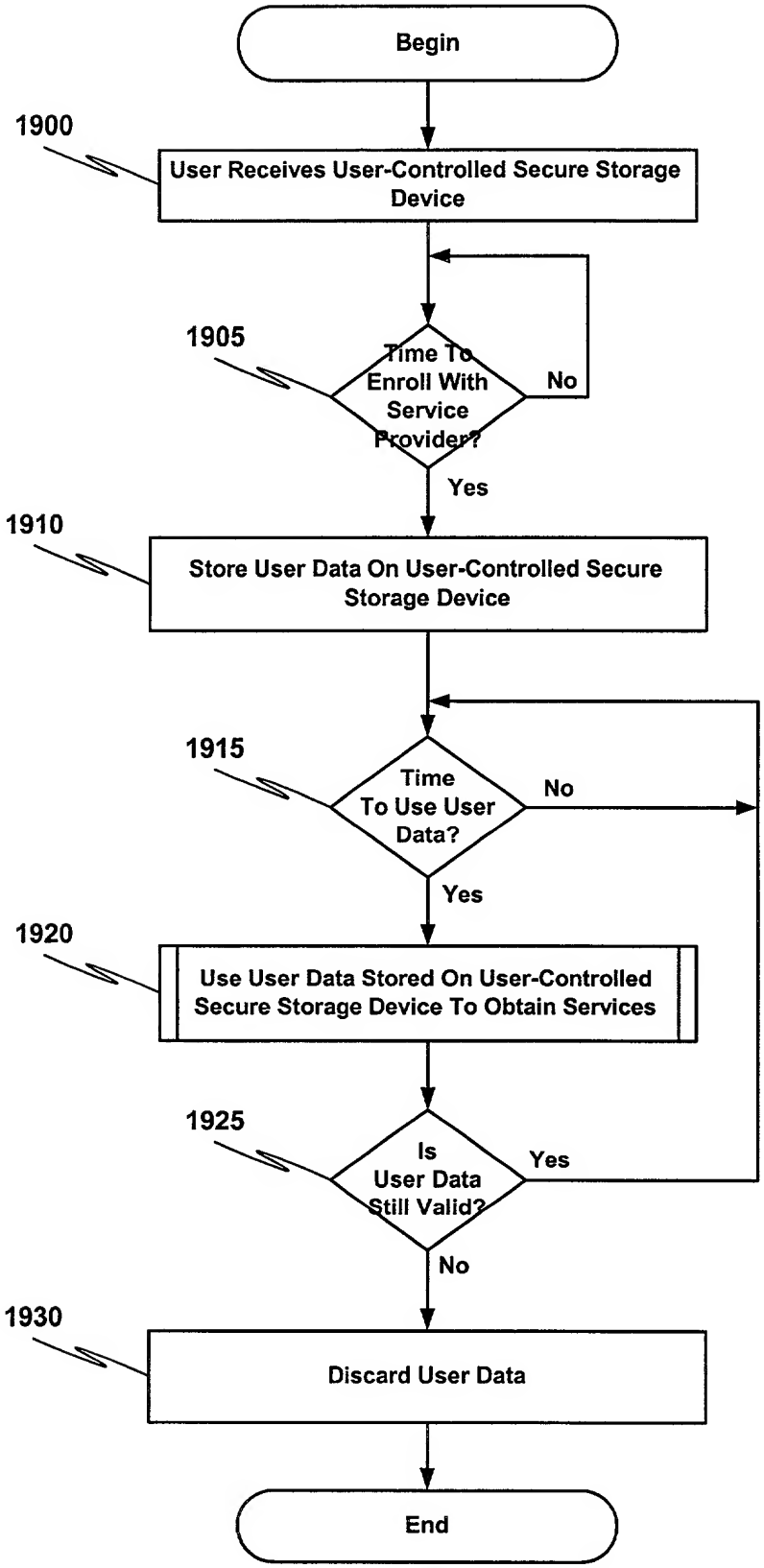
Begin
1900
User Receives User-Controlled Secure Storage Device
1905
Time To Enroll With Service Provider?
No
Yes
1910
Store User Data On User-Controlled Secure Storage Device
1915
Time To Use User Data?
No
Yes
1920
Use User Data Stored On User-Controlled Secure Storage Device To Obtain Services
1925
Is User Data Still Valid?
Yes
No
1930
Discard User Data
End

FIG. 19

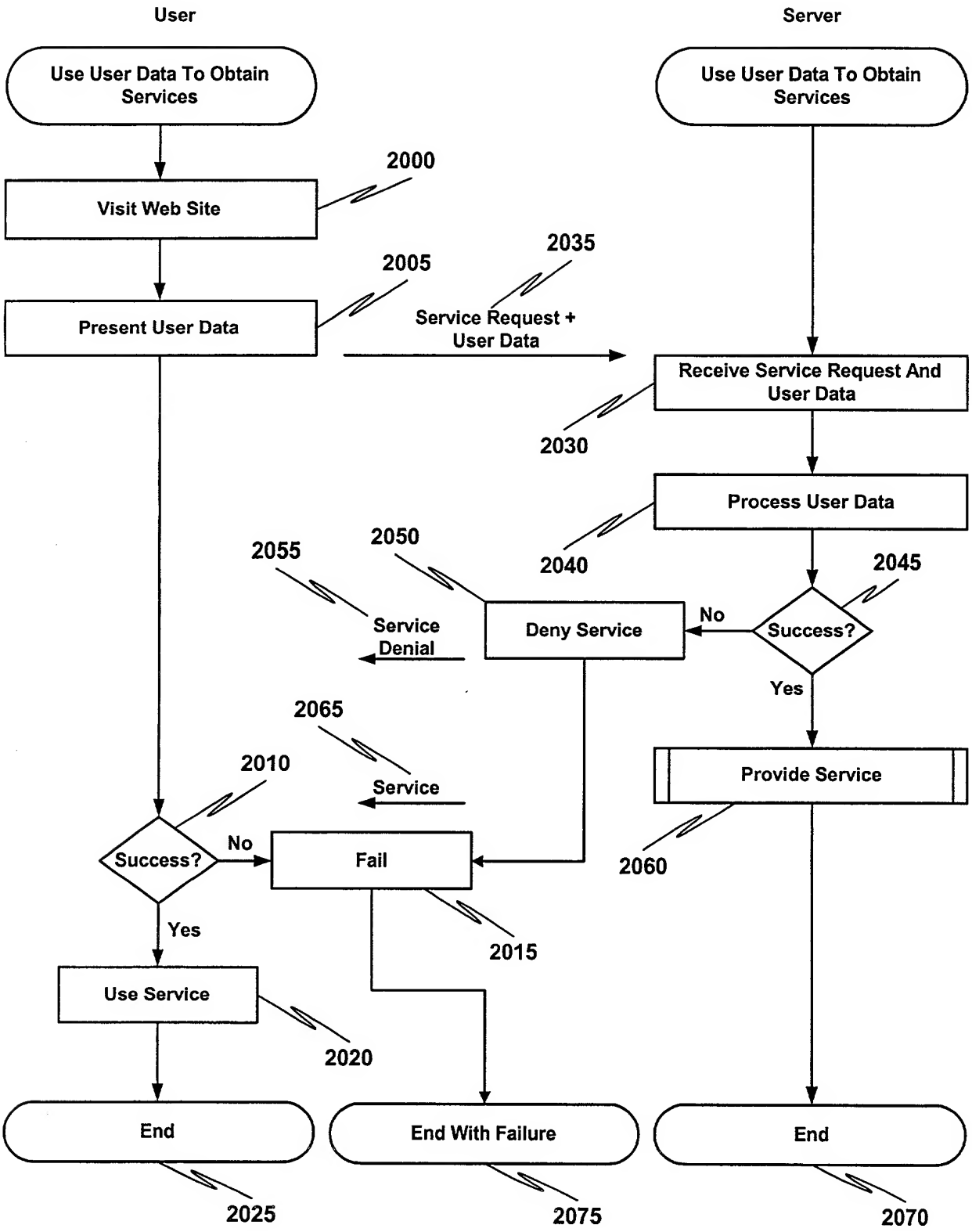
User
Server
Use User Data To Obtain Services
Use User Data To Obtain Services
2000
Visit Web Site
2005
Present User Data
2035
Service Request + User Data
Receive Service Request And User Data
2030
Process User Data
2040
2050
2055
2045
Service Denial
Deny Service
No
Success?
Yes
2065
Service
2010
Provide Service
Success?
No
Fail
2060
Yes
2015
Use Service
2020
End
End With Failure
End
2025
2075
2070

FIG. 20

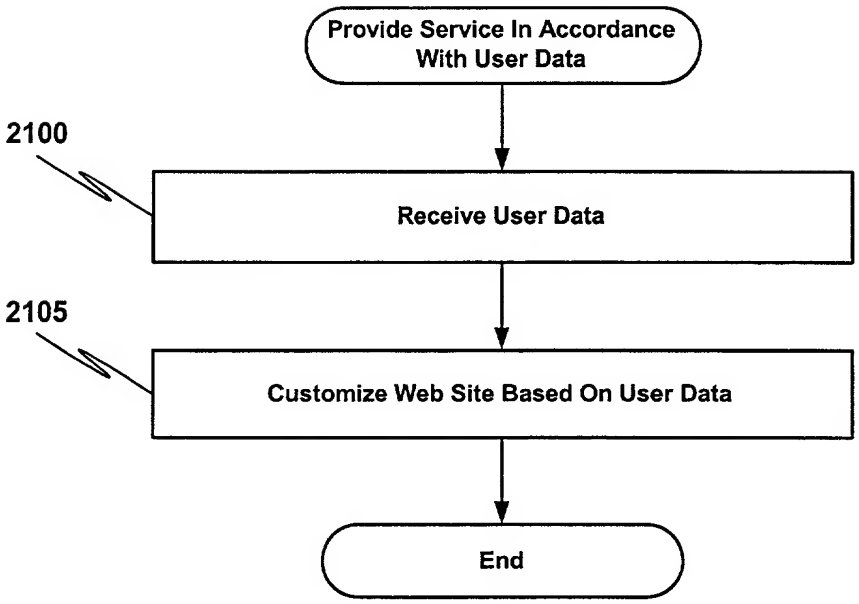
Provide Service In Accordance With User Data
2100
Receive User Data
2105
Customize Web Site Based On User Data
End

FIG. 21

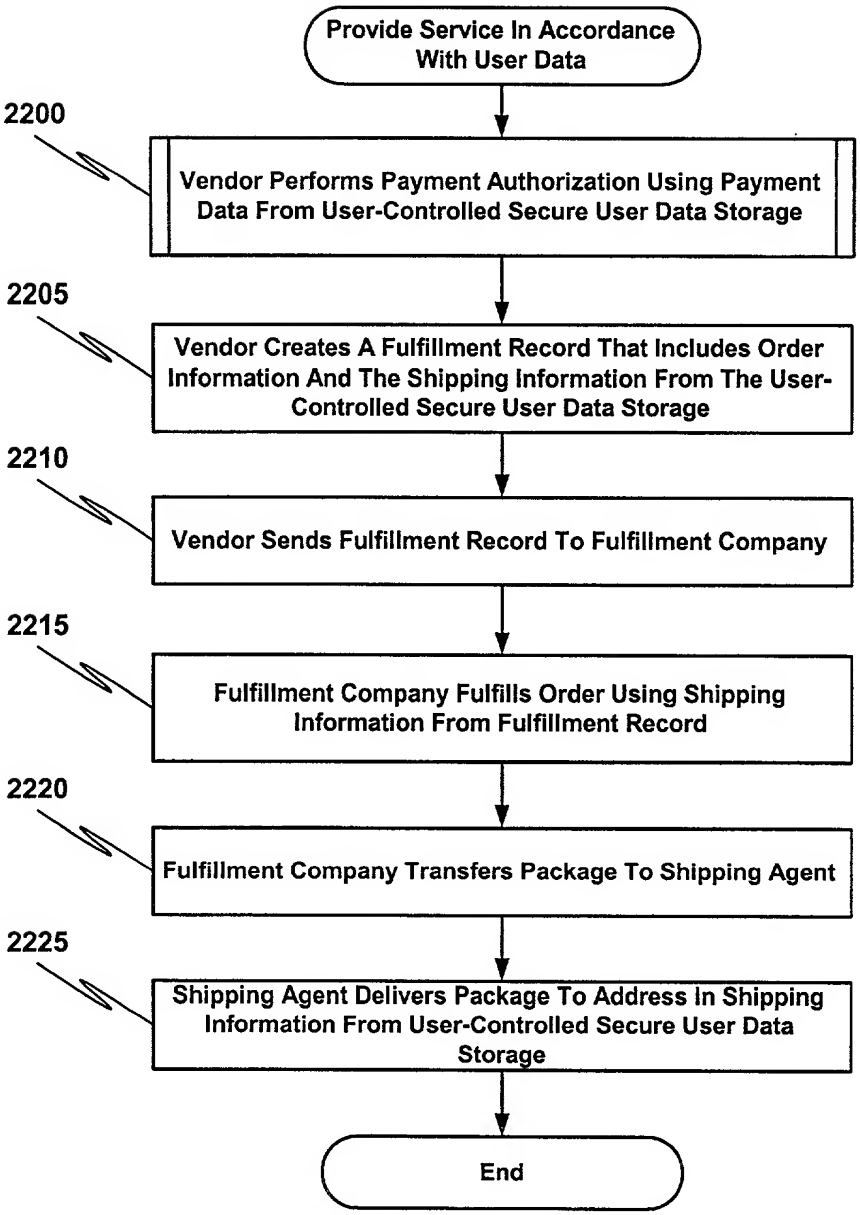
Provide Service In Accordance With User Data
2200
Vendor Performs Payment Authorization Using Payment Data From User-Controlled Secure User Data Storage
2205
Vendor Creates A Fulfillment Record That Includes Order Information And The Shipping Information From The User-Controlled Secure User Data Storage
2210
Vendor Sends Fulfillment Record To Fulfillment Company
2215
Fulfillment Company Fulfills Order Using Shipping Information From Fulfillment Record
2220
Fulfillment Company Transfers Package To Shipping Agent
2225
Shipping Agent Delivers Package To Address In Shipping Information From User-Controlled Secure User Data Storage
End

FIG. 22

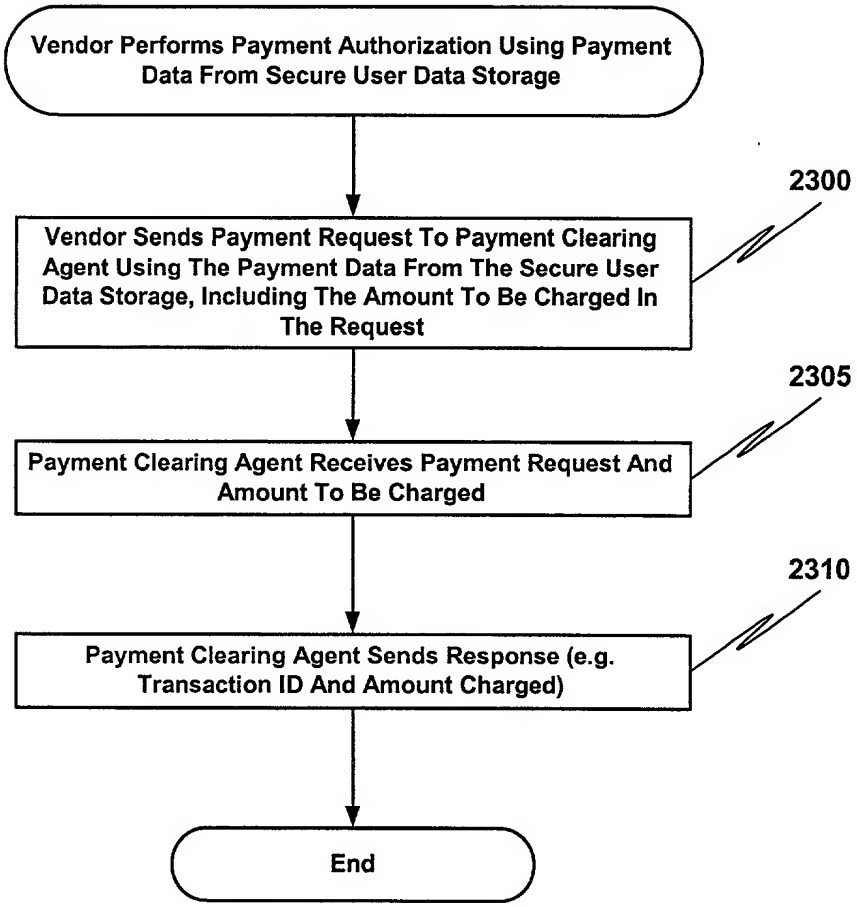
Vendor Performs Payment Authorization Using Payment Data From Secure User Data Storage
2300
Vendor Sends Payment Request To Payment Clearing Agent Using The Payment Data From The Secure User Data Storage, Including The Amount To Be Charged In The Request
2305
Payment Clearing Agent Receives Payment Request And Amount To Be Charged
2310
Payment Clearing Agent Sends Response (e.g. Transaction ID And Amount Charged)
End

FIG. 23

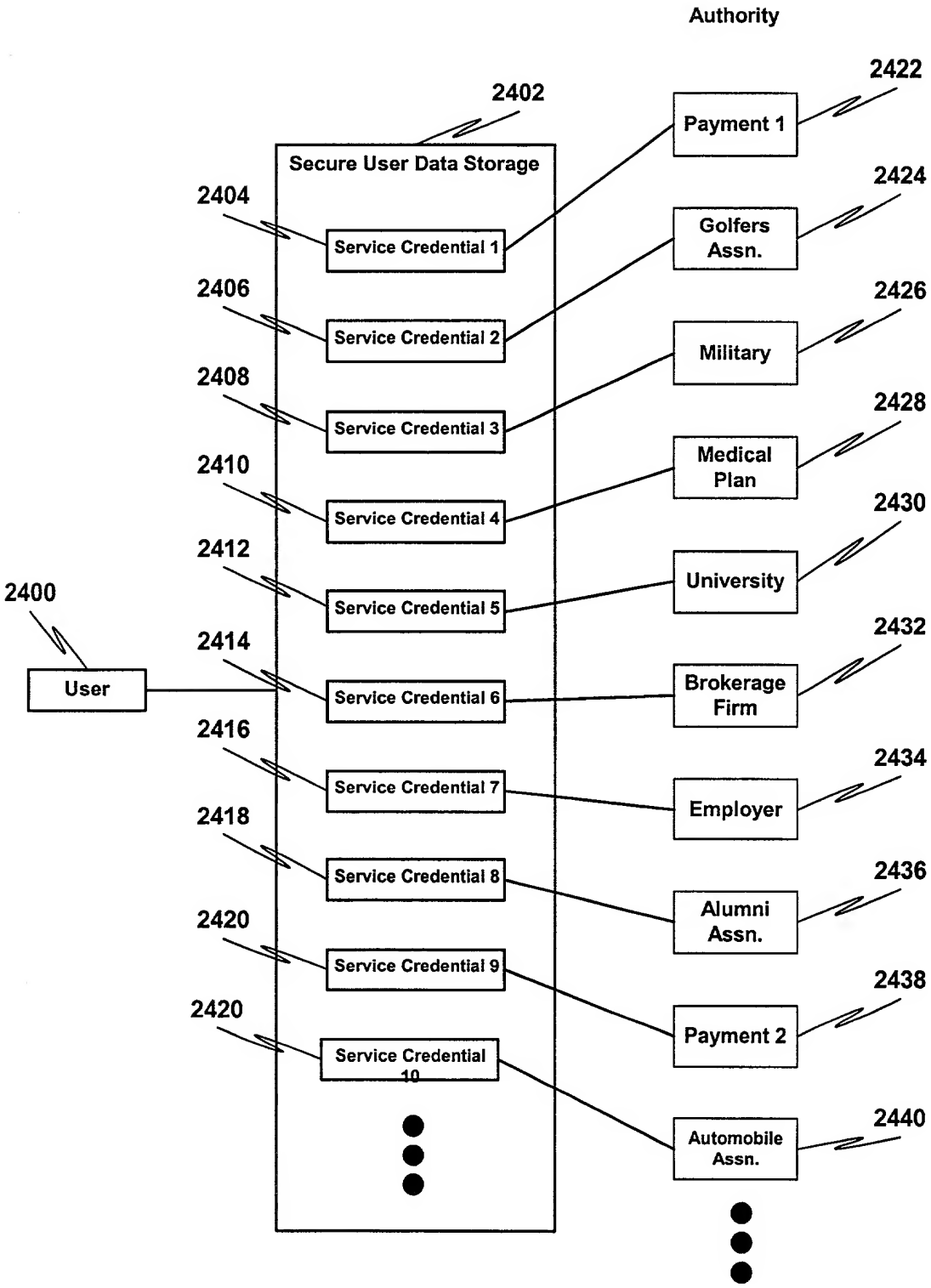
Authority
2402
Secure User Data Storage
2400
User
2404
Service Credential 1
2406
Service Credential 2
2408
Service Credential 3
2410
Service Credential 4
2412
Service Credential 5
2414
Service Credential 6
2416
Service Credential 7
2418
Service Credential 8
2420
Service Credential 9
2420
Service Credential 10
2422
Payment 1
2424
Golfers Assn.
2426
Military
2428
Medical Plan
2430
University
2432
Brokerage Firm
2434
Employer
2436
Alumni Assn.
2438
Payment 2
2440
Automobile Assn.

FIG. 24

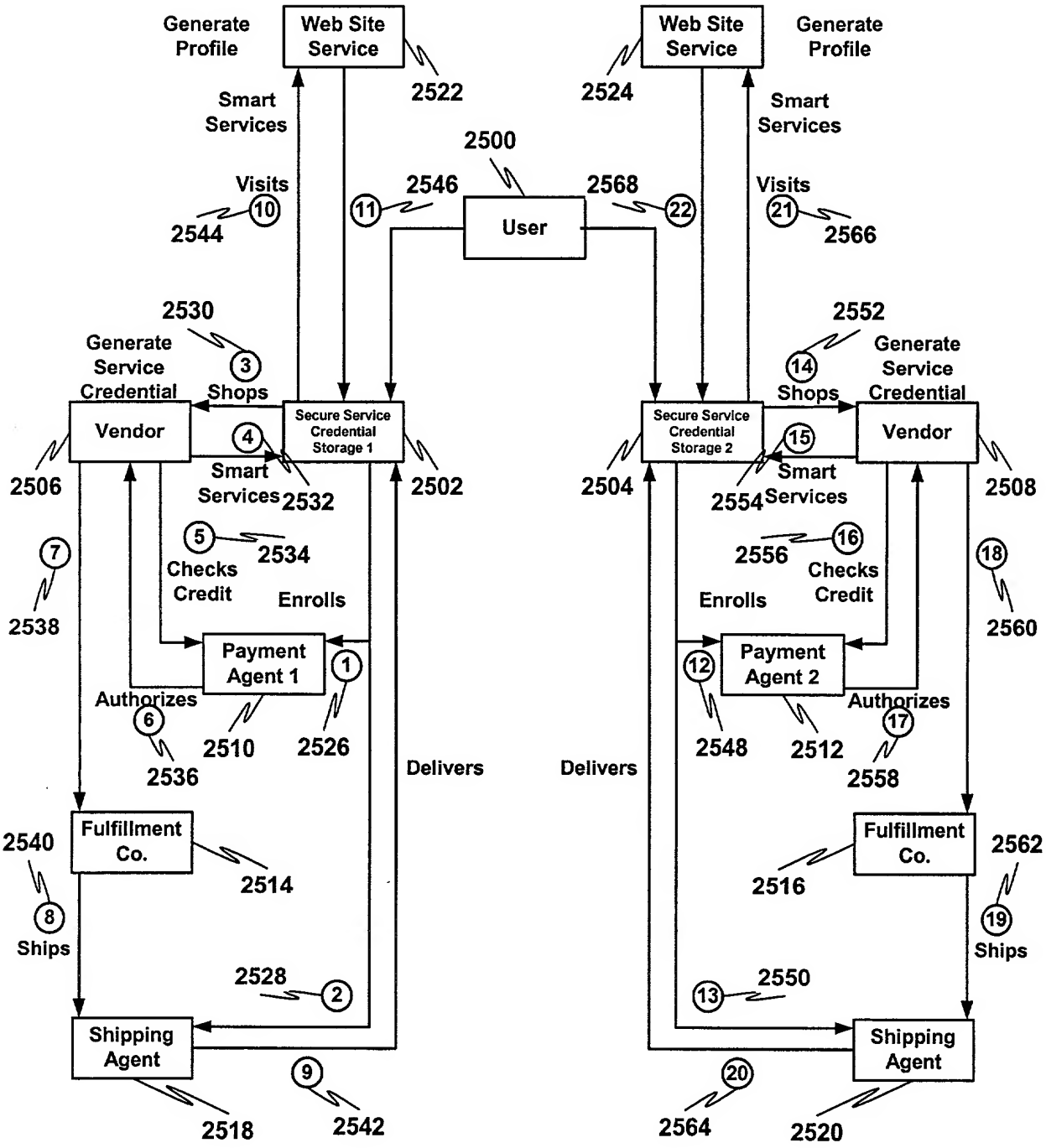
Generate Profile
Web Site Service
2522
2524
Web Site Service
Generate Profile
Smart Services
2500
Visits
10
2544
2546
11
User
2568
22
Visits
21
2566
Smart Services
2530
Generate Service Credential
3
Shops
Vendor
2506
4
Smart Services
2532
Secure Service Credential Storage 1
2502
Secure Service Credential Storage 2
2504
2552
14
Shops
Generate Service Credential
Vendor
2508
15
Smart Services
2554
5
Checks Credit
2534
Enrolls
2556
16
Checks Credit
7
2538
18
2560
Payment Agent 1
1
Authorizes
6
2536
2510
2526
Payment Agent 2
12
2548
2512
Authorizes
17
2558
Delivers
Delivers
Fulfillment Co.
2540
2514
Fulfillment Co.
2516
2562
8
Ships
19
Ships
2528
2
2550
13
Shipping Agent
9
2542
2518
Shipping Agent
20
2564
2520

FIG. 25

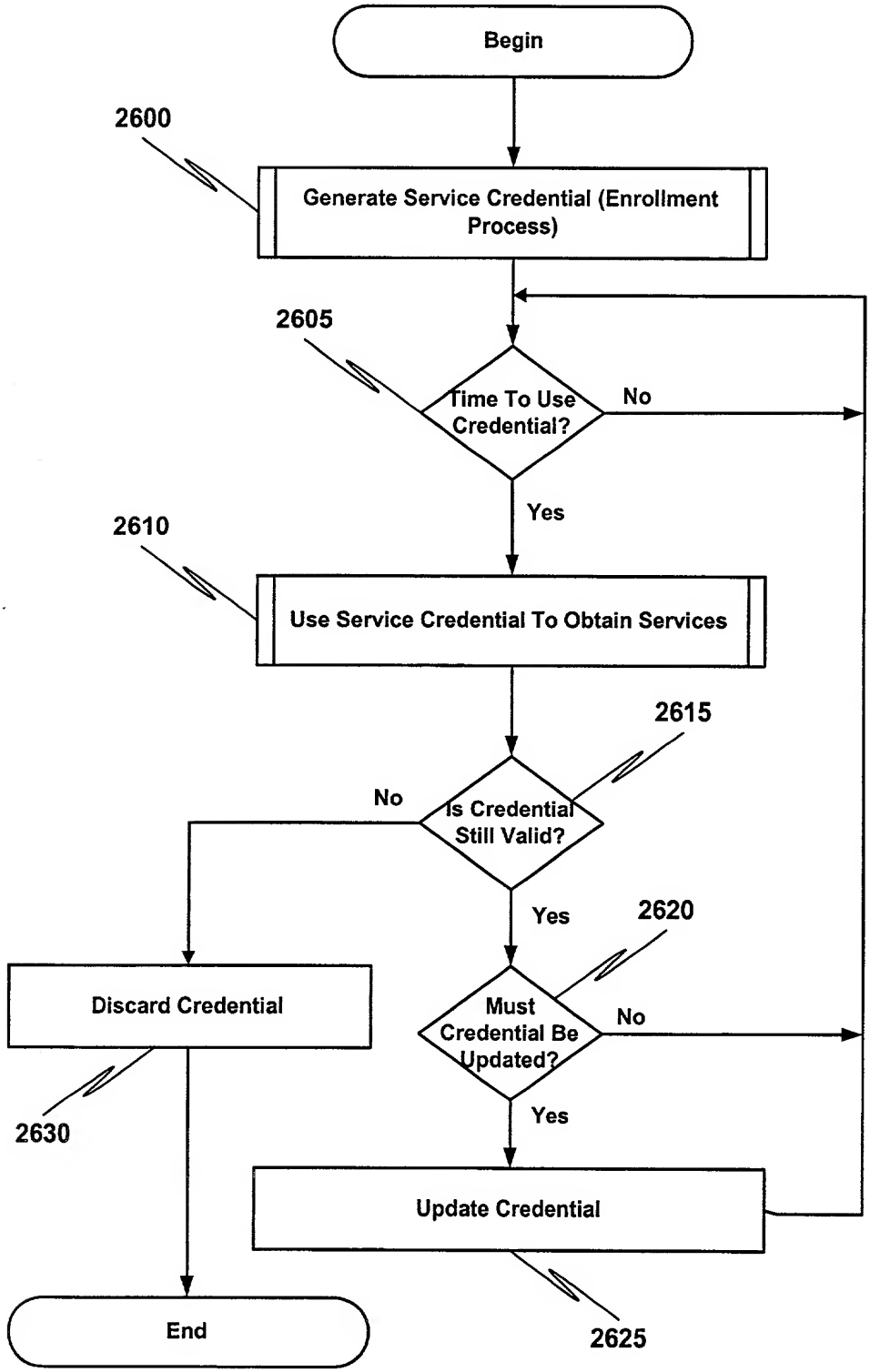
Begin
2600
Generate Service Credential (Enrollment Process)
2605
Time To Use Credential?
No
Yes
2610
Use Service Credential To Obtain Services
2615
Is Credential Still Valid?
No
Yes
2620
Must Credential Be Updated?
No
Yes
Discard Credential
2630
Update Credential
2625
End

FIG. 26

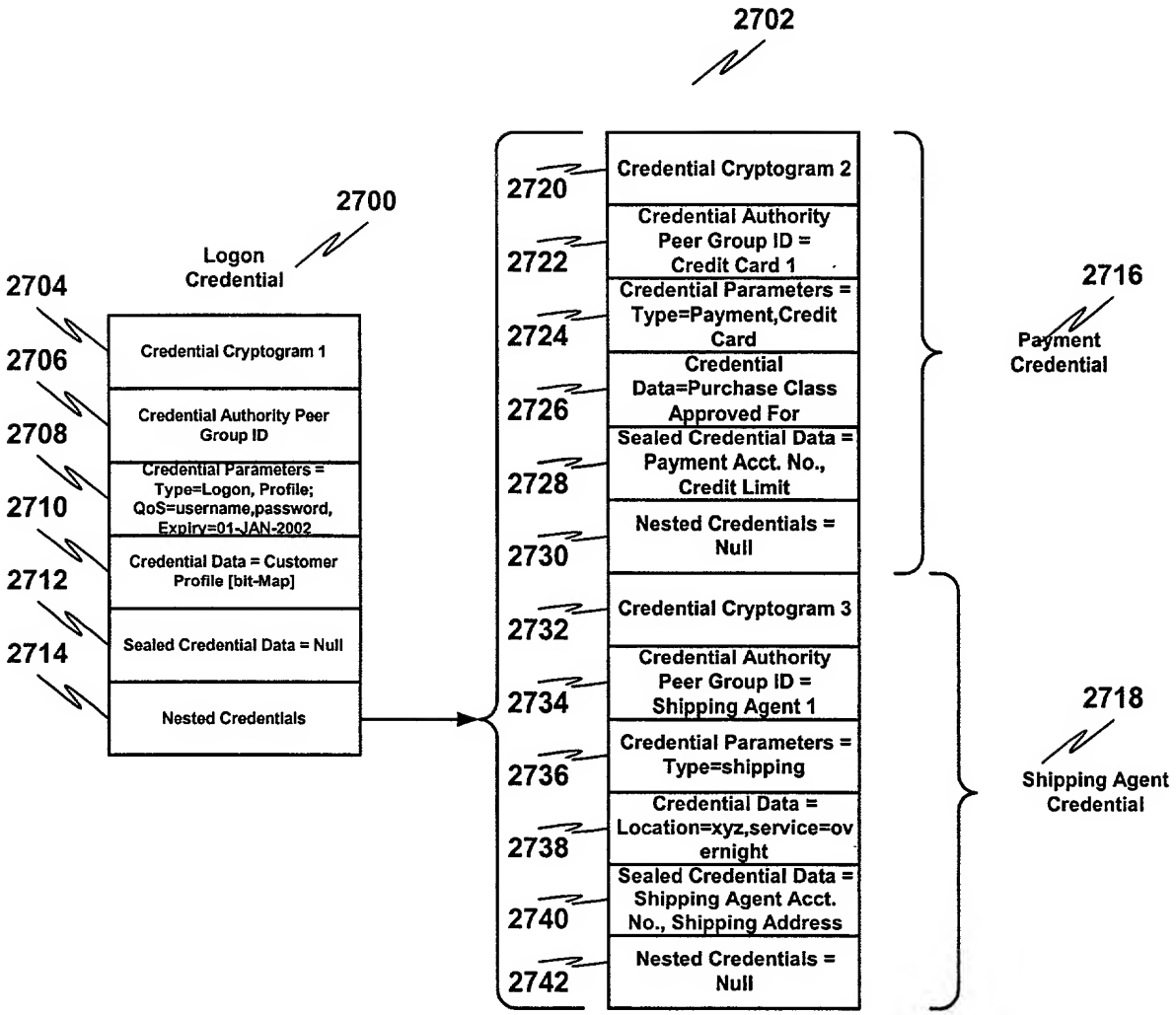
2702
2700
Logon Credential
2704
2706
2708
2710
2712
2714
Credential Cryptogram 1
Credential Authority Peer Group ID
Credential Parameters = Type=Logon, Profile; QoS=username,password, Expiry=01-JAN-2002
Credential Data = Customer Profile [bit-Map]
Sealed Credential Data = Null
Nested Credentials
2720
2722
2724
2726
2728
2730
2732
2734
2736
2738
2740
2742
Credential Cryptogram 2
Credential Authority Peer Group ID = Credit Card 1
Credential Parameters = Type=Payment,Credit Card
Credential Data=Purchase Class Approved For
Sealed Credential Data = Payment Acct. No., Credit Limit
Nested Credentials = Null
Credential Cryptogram 3
Credential Authority Peer Group ID = Shipping Agent 1
Credential Parameters = Type=shipping
Credential Data = Location=xyz,service=overnight
Sealed Credential Data = Shipping Agent Acct. No., Shipping Address
Nested Credentials = Null
2716
Payment Credential
2718
Shipping Agent Credential

FIG. 27

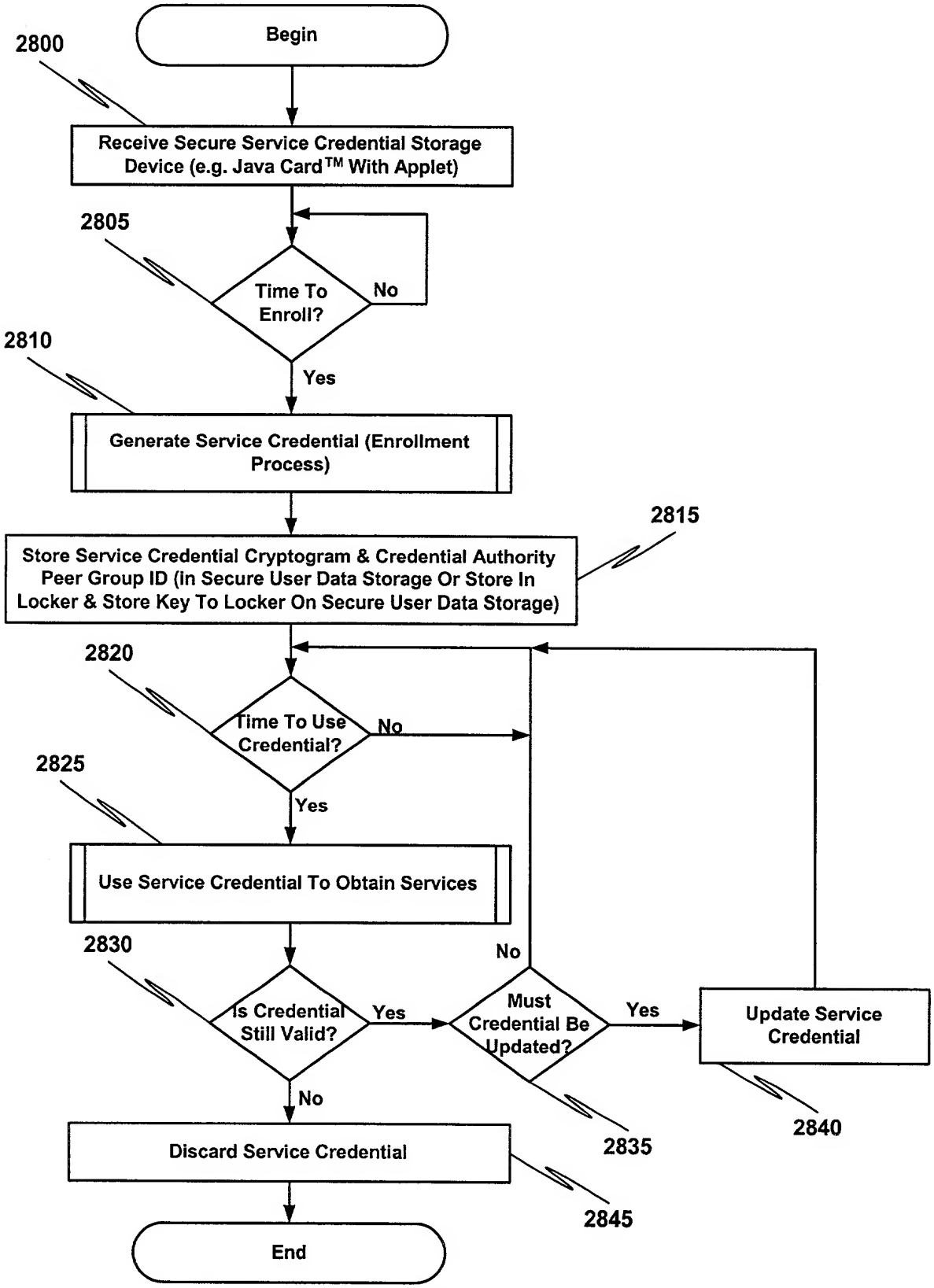
Begin
2800
Receive Secure Service Credential Storage Device (e.g. Java Card™ With Applet)
2805
Time To Enroll?
No
Yes
2810
Generate Service Credential (Enrollment Process)
2815
Store Service Credential Cryptogram & Credential Authority Peer Group ID (in Secure User Data Storage Or Store In Locker & Store Key To Locker On Secure User Data Storage)
2820
Time To Use Credential?
No
Yes
2825
Use Service Credential To Obtain Services
2830
Is Credential Still Valid?
Yes
No
Must Credential Be Updated?
Yes
No
Update Service Credential
2835
2840
Discard Service Credential
2845
End

FIG. 28A

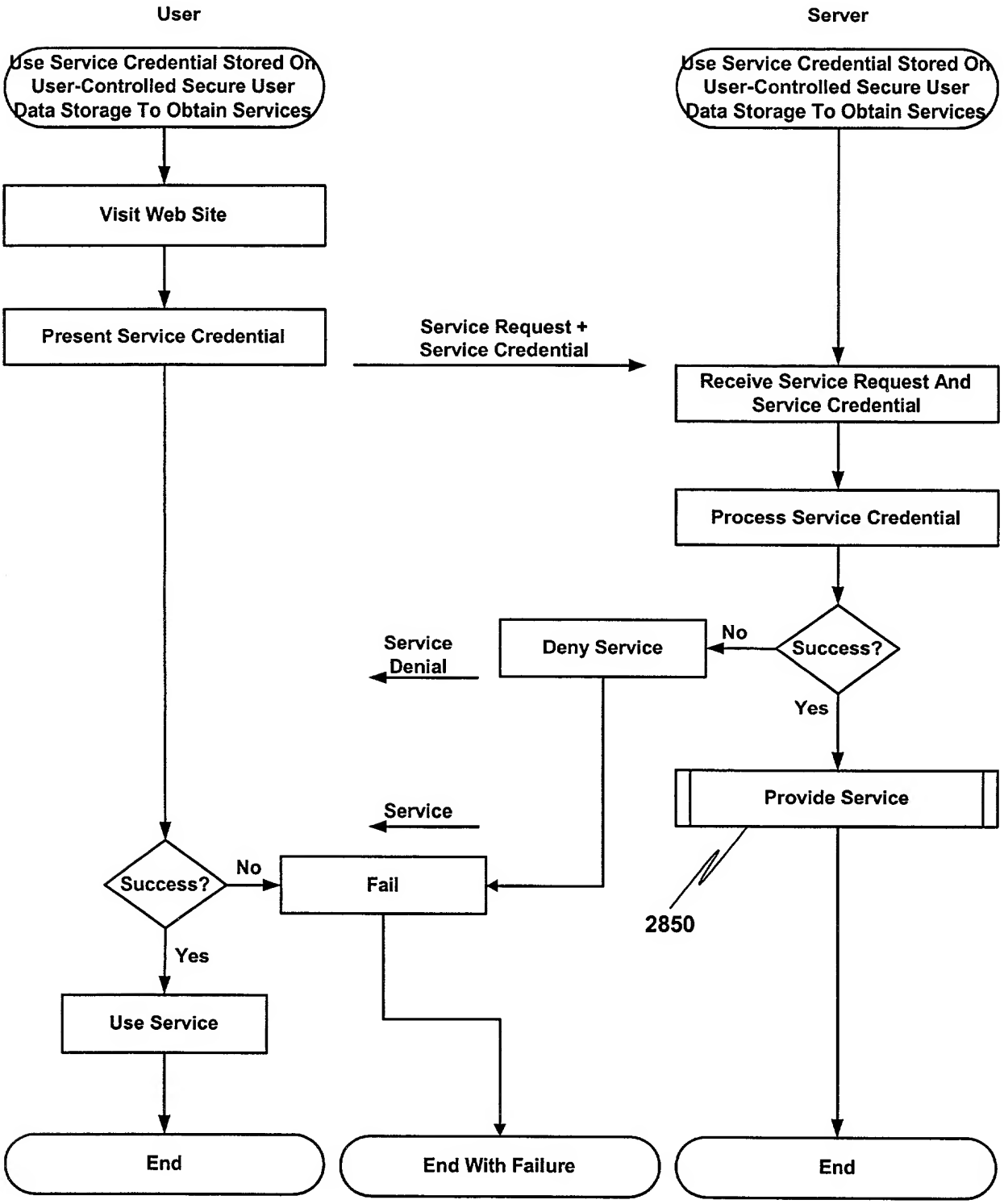
User
Server
Use Service Credential Stored On User-Controlled Secure User Data Storage To Obtain Services
Use Service Credential Stored On User-Controlled Secure User Data Storage To Obtain Services
Visit Web Site
Present Service Credential
Service Request + Service Credential
Receive Service Request And Service Credential
Process Service Credential
Success?
No
Deny Service
Service Denial
Yes
Provide Service
Service
Success?
No
Fail
2850
Yes
Use Service
End
End With Failure
End

FIG. 28B

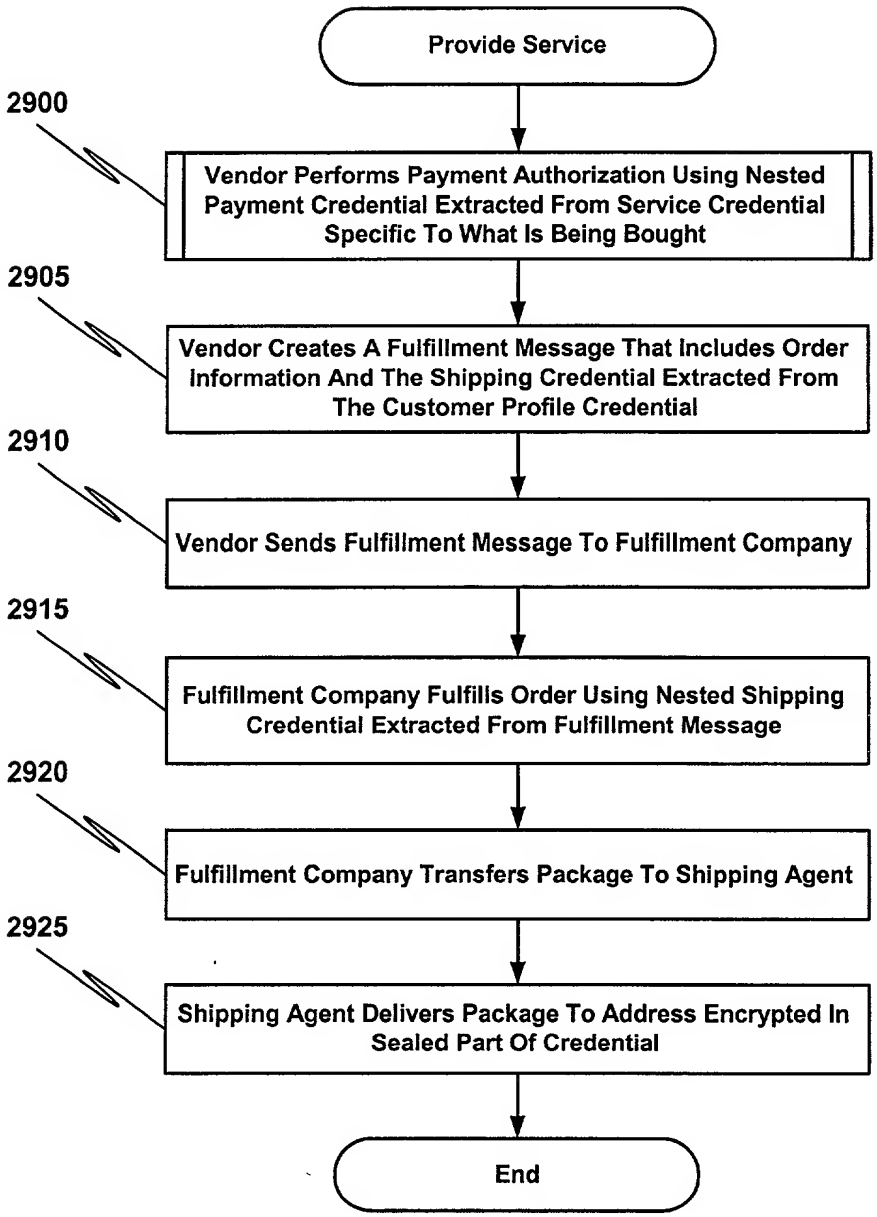
Provide Service
2900
Vendor Performs Payment Authorization Using Nested Payment Credential Extracted From Service Credential Specific To What Is Being Bought
2905
Vendor Creates A Fulfillment Message That Includes Order Information And The Shipping Credential Extracted From The Customer Profile Credential
2910
Vendor Sends Fulfillment Message To Fulfillment Company
2915
Fulfillment Company Fulfills Order Using Nested Shipping Credential Extracted From Fulfillment Message
2920
Fulfillment Company Transfers Package To Shipping Agent
2925
Shipping Agent Delivers Package To Address Encrypted In Sealed Part Of Credential
End

FIG. 29

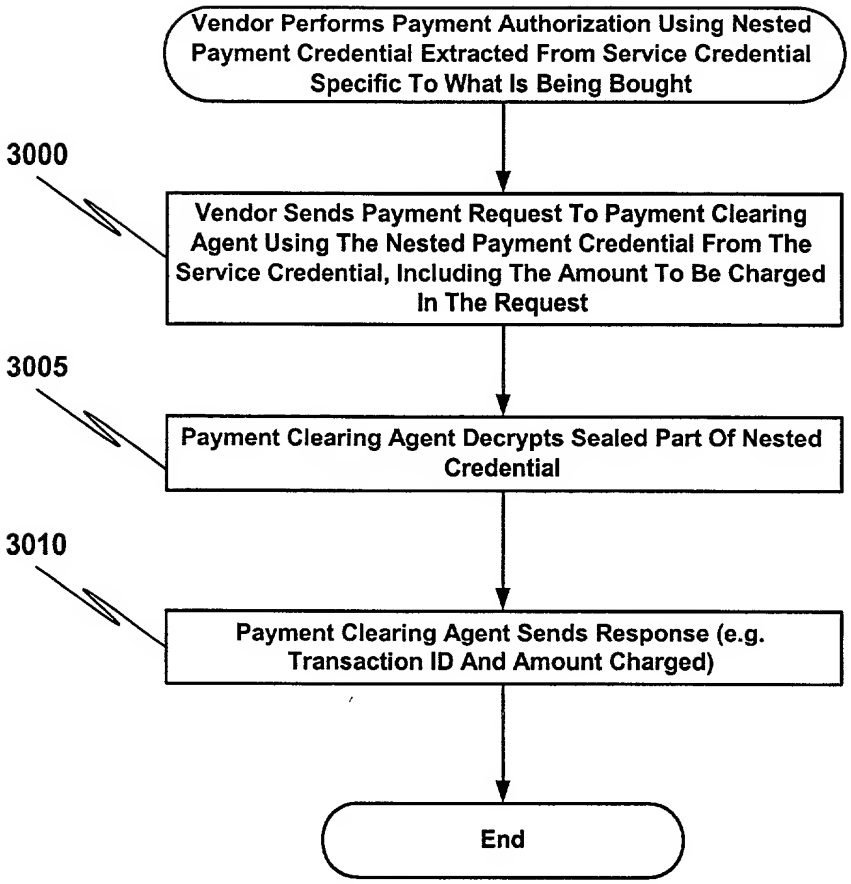
Vendor Performs Payment Authorization Using Nested Payment Credential Extracted From Service Credential Specific To What Is Being Bought
3000
Vendor Sends Payment Request To Payment Clearing Agent Using The Nested Payment Credential From The Service Credential, Including The Amount To Be Charged In The Request
3005
Payment Clearing Agent Decrypts Sealed Part Of Nested Credential
3010
Payment Clearing Agent Sends Response (e.g. Transaction ID And Amount Charged)
End

FIG. 30A

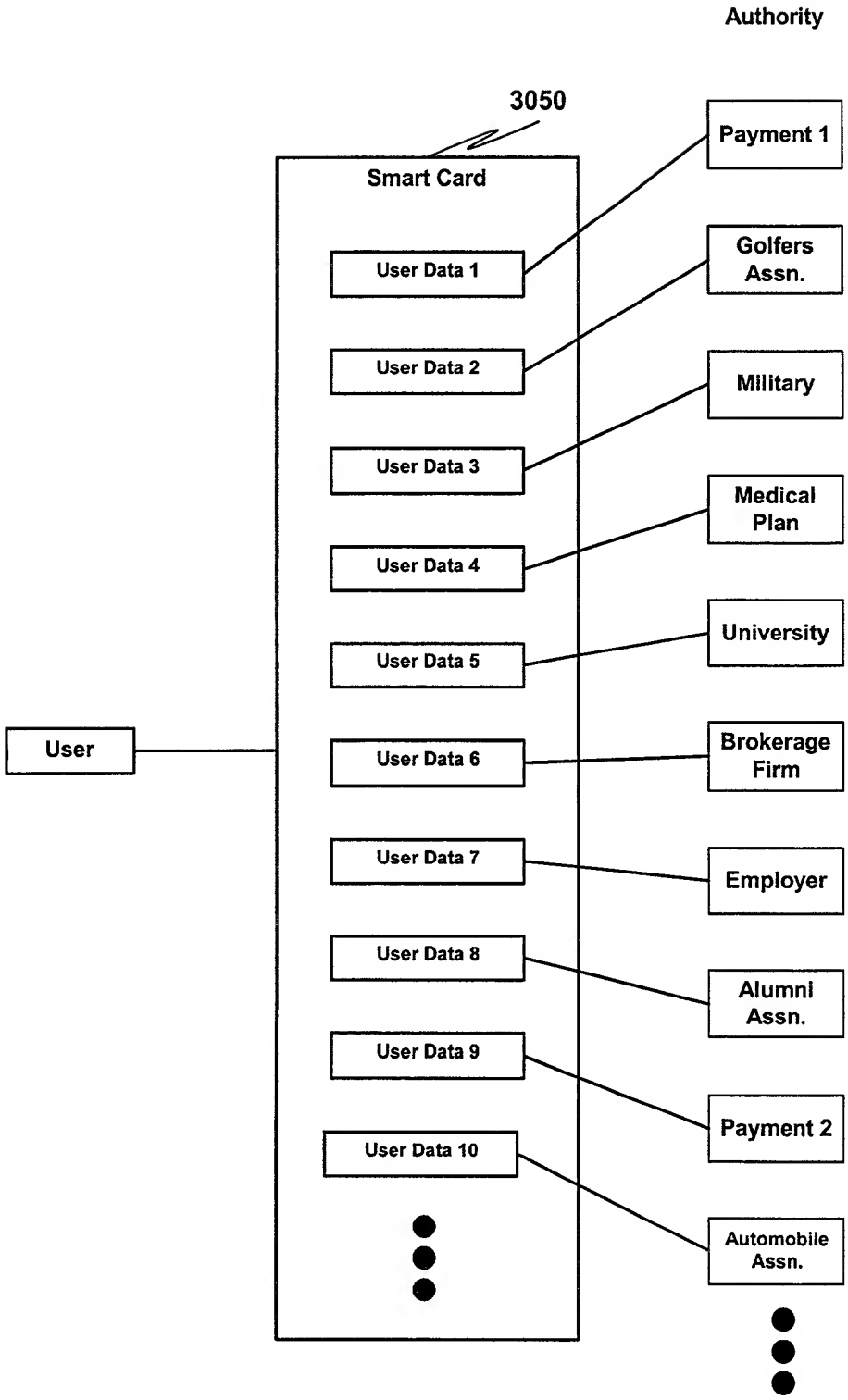
Authority
3050
Smart Card
User
User Data 1
User Data 2
User Data 3
User Data 4
User Data 5
User Data 6
User Data 7
User Data 8
User Data 9
User Data 10
Payment 1
Golfers Assn.
Military
Medical Plan
University
Brokerage Firm
Employer
Alumni Assn.
Payment 2
Automobile Assn.

FIG. 30B

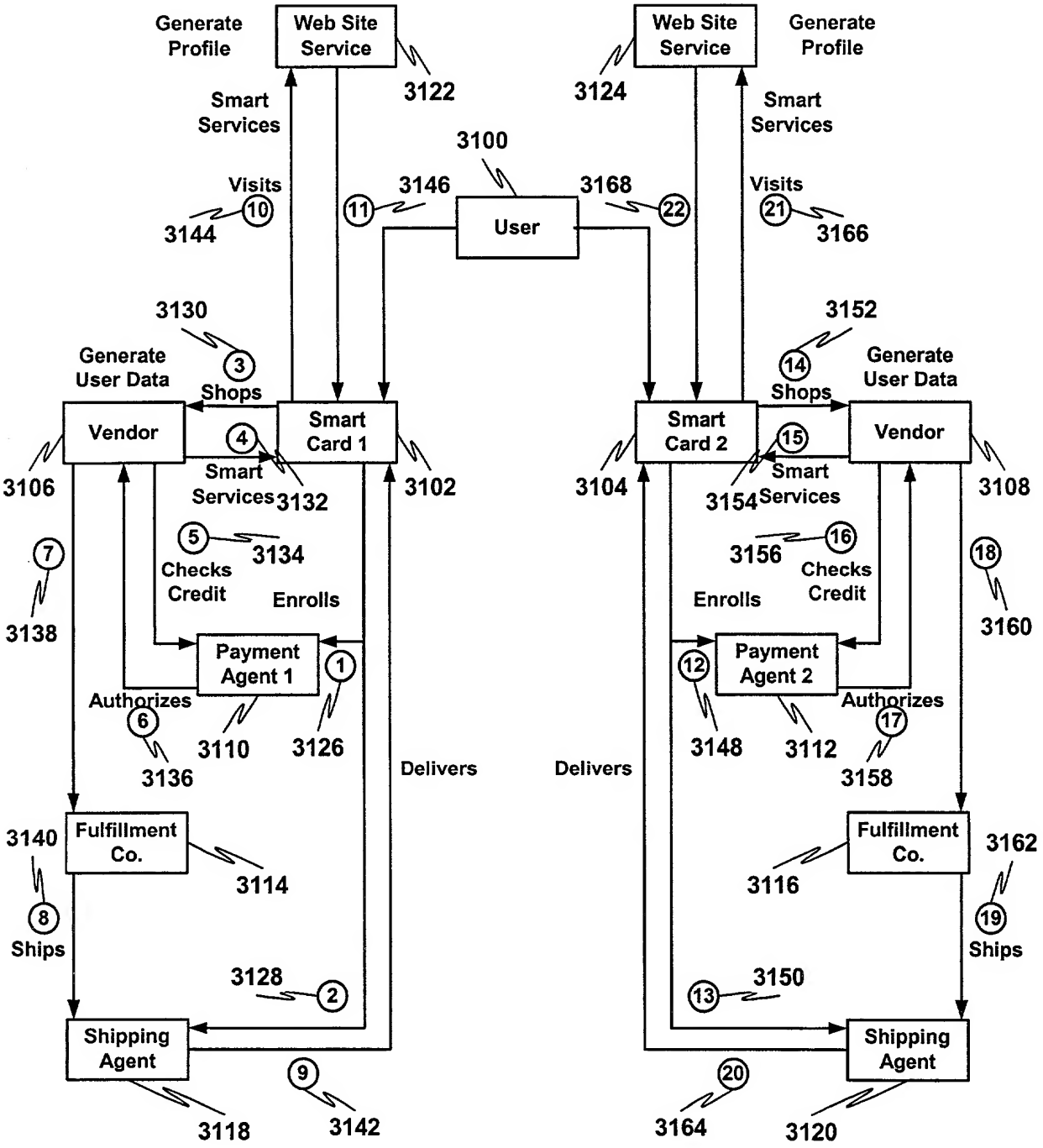
Generate Profile
Web Site Service
3122
3124
Web Site Service
Generate Profile
Smart Services
Smart Services
3100
Visits
10
3144
11
3146
3168
22
Visits
21
3166
User
3130
3152
Generate User Data
3
Shops
14
Shops
Generate User Data
Vendor
Smart Card 1
Smart Card 2
Vendor
4
15
3106
3102
3104
3108
Smart Services
3132
3154
Smart Services
5
3134
3156
16
7
18
Checks Credit
Enrolls
Enrolls
Checks Credit
3138
3160
Payment Agent 1
Payment Agent 2
12
1
Authorizes
Authorizes
6
17
3110
3126
3148
3112
3136
3158
Delivers
Delivers
3140
Fulfillment Co.
Fulfillment Co.
3162
3114
3116
8
19
Ships
Ships
3128
2
3150
13
Shipping Agent
Shipping Agent
9
20
3118
3142
3164
3120

FIG. 31

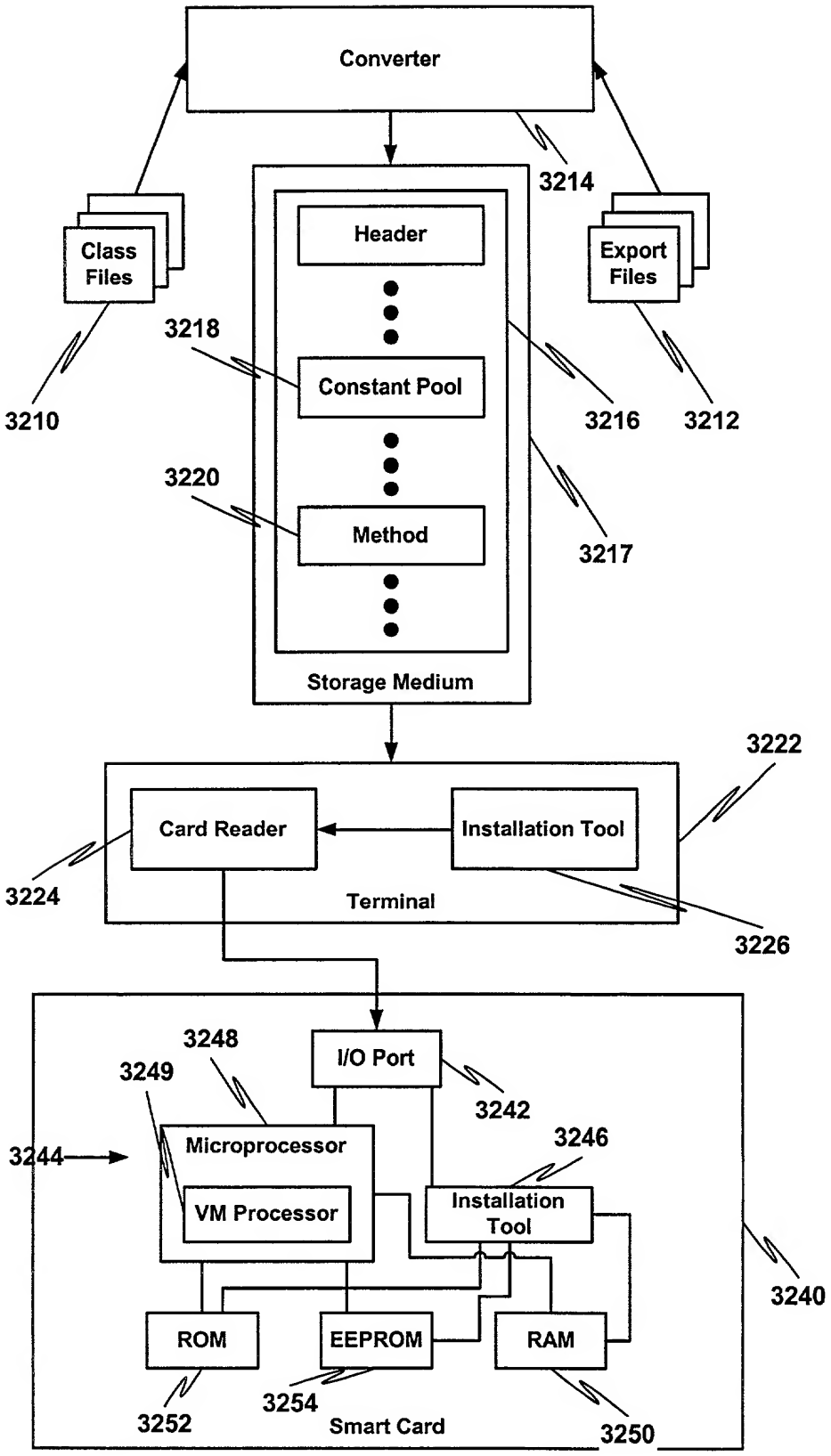
Converter
3214
Class Files
Export Files
Header
3218
Constant Pool
3210
3216
3212
3220
Method
3217
Storage Medium
3222
Card Reader
Installation Tool
3224
Terminal
3226
3248
I/O Port
3249
3242
Microprocessor
3246
3244
VM Processor
Installation Tool
3240
ROM
EEPROM
RAM
3252
3254
Smart Card
3250

FIG. 32

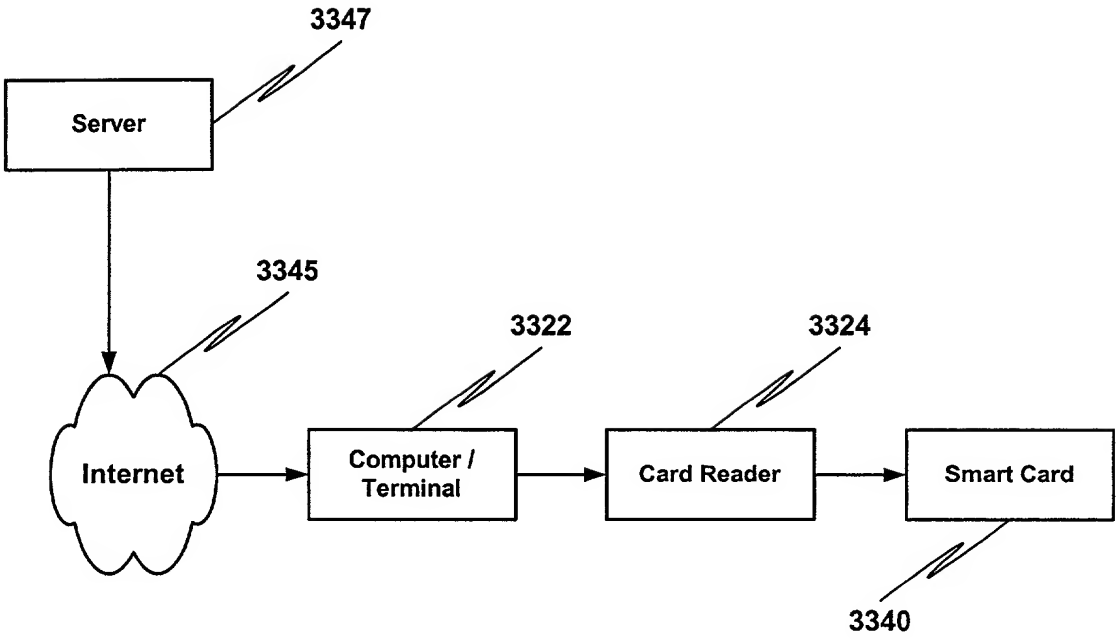
3347
Server
3345
3322
3324
Internet
Computer / Terminal
Card Reader
Smart Card
3340

FIG. 33A

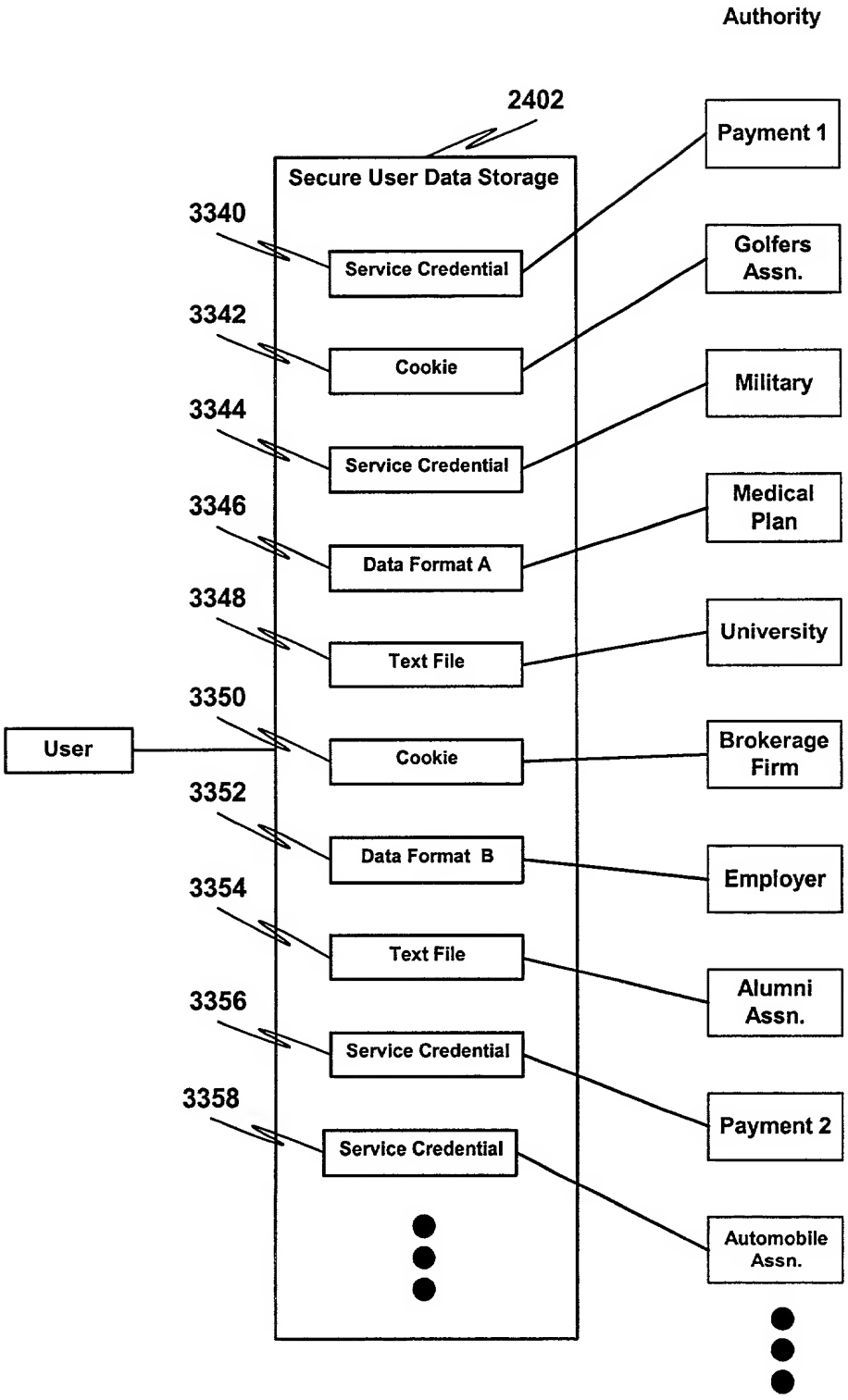
Authority
2402
Secure User Data Storage
3340
Service Credential
3342
Cookie
3344
Service Credential
3346
Data Format A
3348
Text File
3350
Cookie
3352
Data Format B
3354
Text File
3356
Service Credential
3358
Service Credential
User
Payment 1
Golfers Assn.
Military
Medical Plan
University
Brokerage Firm
Employer
Alumni Assn.
Payment 2
Automobile Assn.

FIG. 33B

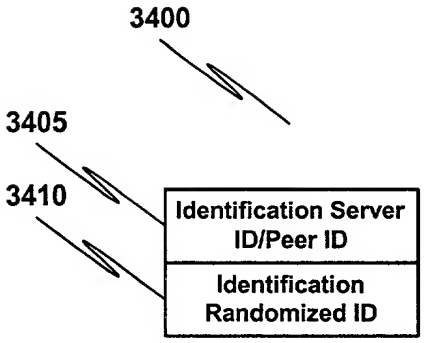
3400
3405
3410
Identification Server ID/Peer ID
Identification Randomized ID

FIG. 34

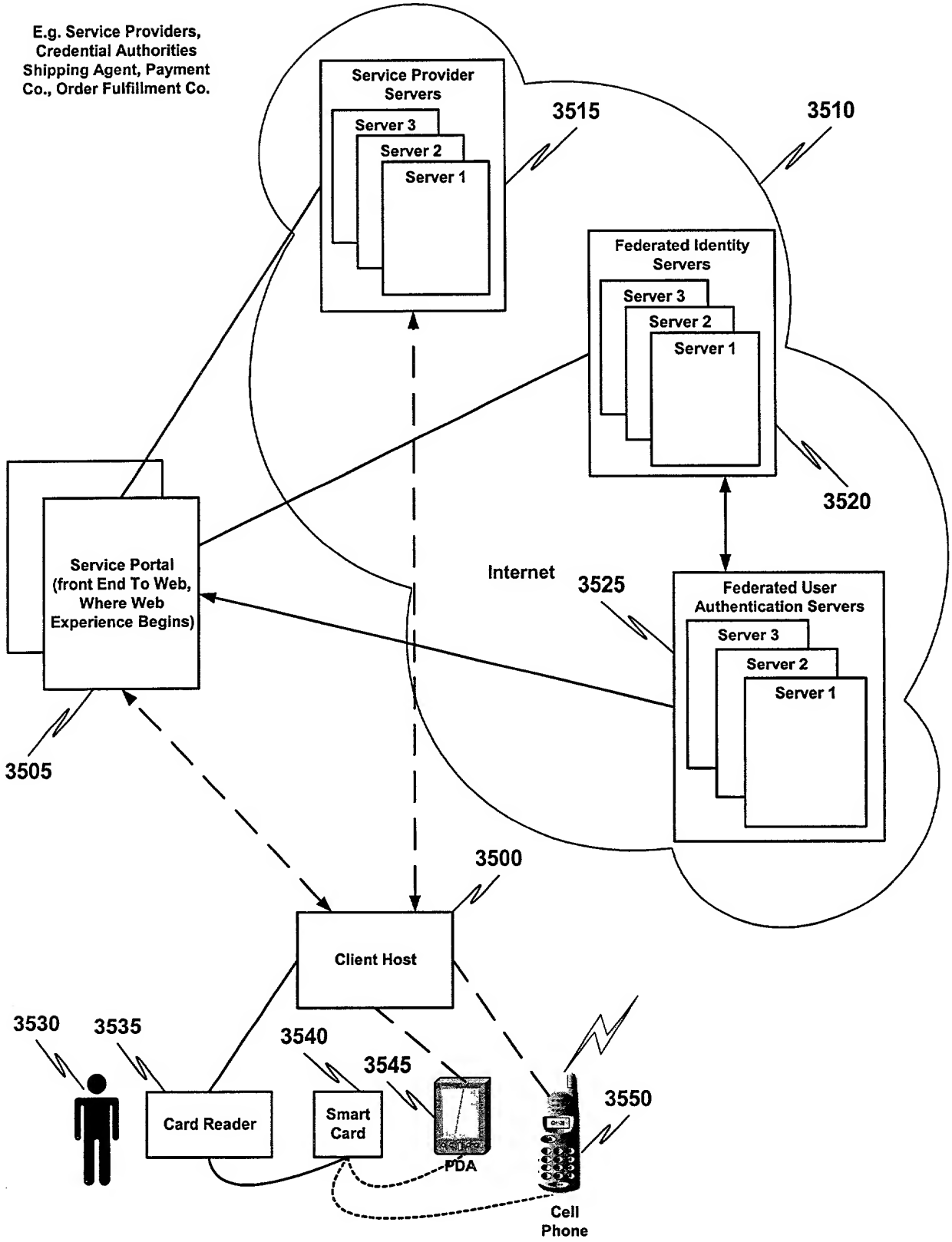
E.g. Service Providers, Credential Authorities Shipping Agent, Payment Co., Order Fulfillment Co.
Service Provider Servers
Server 3
Server 2
Server 1
3515
3510
Federated Identity Servers
Server 3
Server 2
Server 1
3520
Service Portal (front End To Web, Where Web Experience Begins)
Internet
3525
Federated User Authentication Servers
Server 3
Server 2
Server 1
3505
3500
Client Host
3530
3535
3540
3545
3550
Card Reader
Smart Card
PDA
Cell Phone

FIG. 35

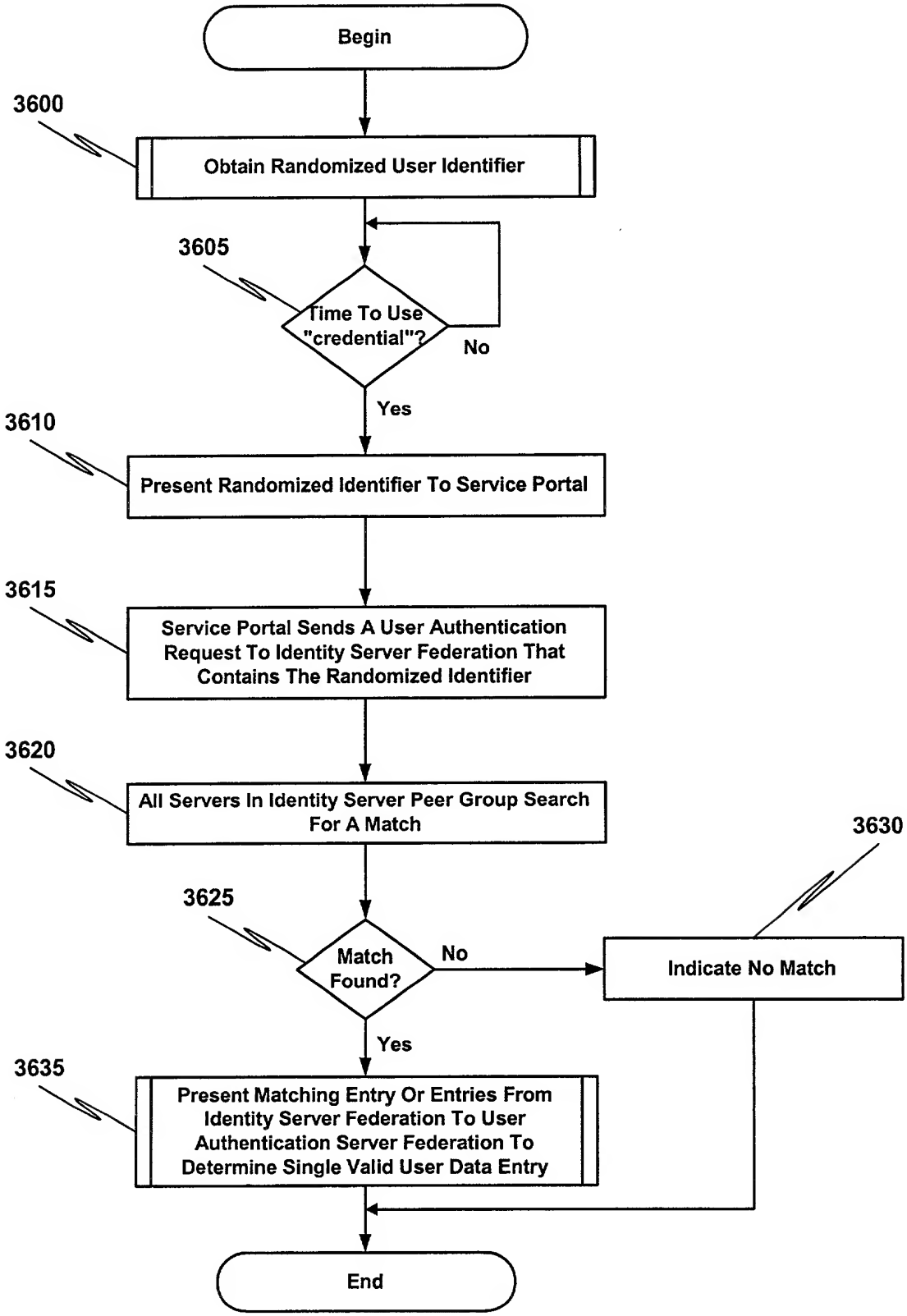
Begin
3600
Obtain Randomized User Identifier
3605
Time To Use "credential"?
No
Yes
3610
Present Randomized Identifier To Service Portal
3615
Service Portal Sends A User Authentication Request To Identity Server Federation That Contains The Randomized Identifier
3620
All Servers In Identity Server Peer Group Search For A Match
3625
Match Found?
No
3630
Indicate No Match
Yes
3635
Present Matching Entry Or Entries From Identity Server Federation To User Authentication Server Federation To Determine Single Valid User Data Entry
End

FIG. 36

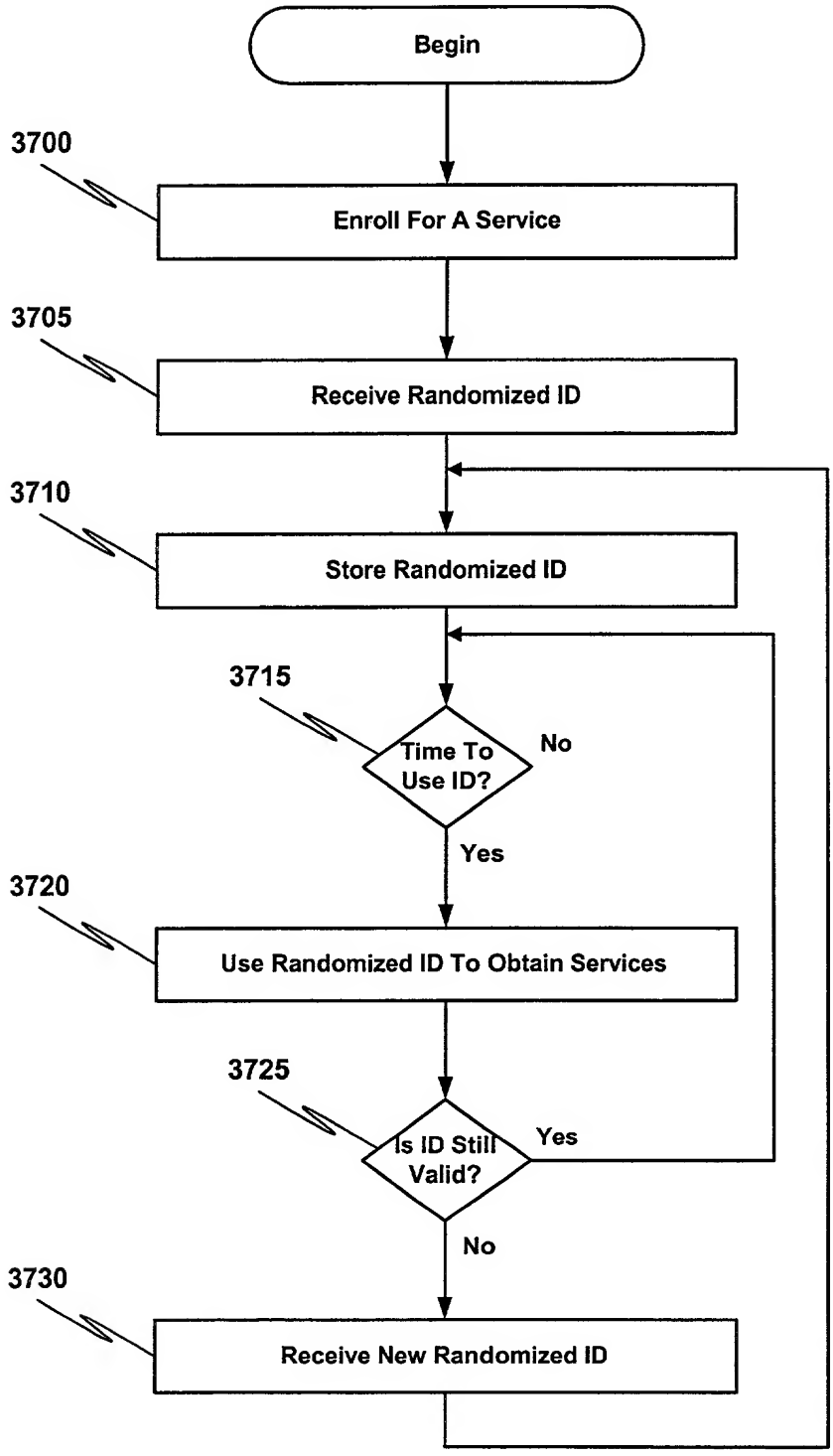
Begin
3700
Enroll For A Service
3705
Receive Randomized ID
3710
Store Randomized ID
3715
Time To Use ID?
No
Yes
3720
Use Randomized ID To Obtain Services
3725
Is ID Still Valid?
Yes
No
3730
Receive New Randomized ID

FIG. 37

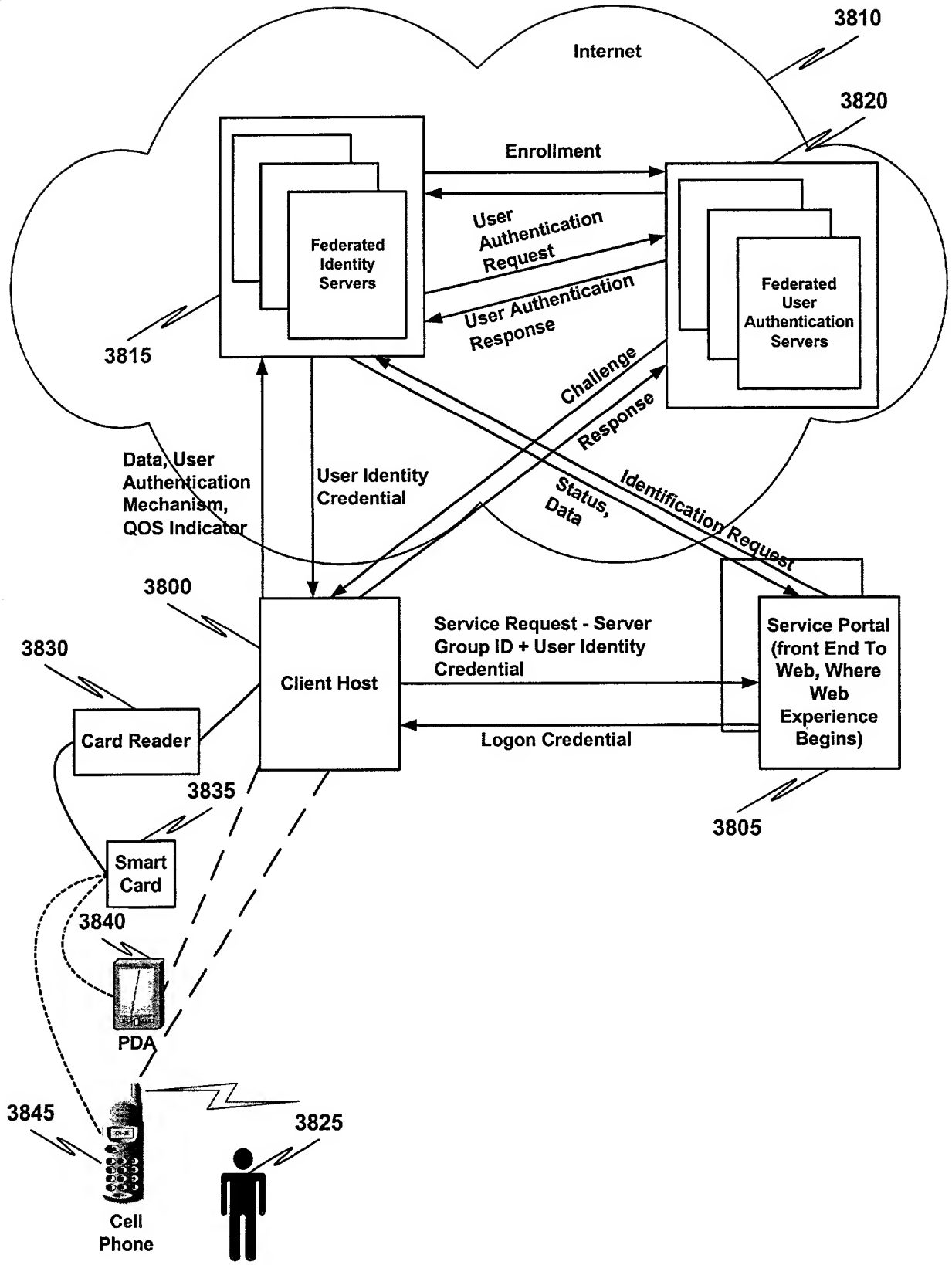
3810
Internet
3820
Enrollment
User Authentication Request
User Authentication Response
Federated Identity Servers
Federated User Authentication Servers
3815
Challenge
Response
Data, User Authentication Mechanism, QOS Indicator
User Identity Credential
Status, Data
Identification Request
3800
Service Request - Server Group ID + User Identity Credential
Logon Credential
Client Host
Service Portal (front End To Web, Where Web Experience Begins)
3830
Card Reader
3835
3805
Smart Card
3840
PDA
3845
3825
Cell Phone

FIG. 38

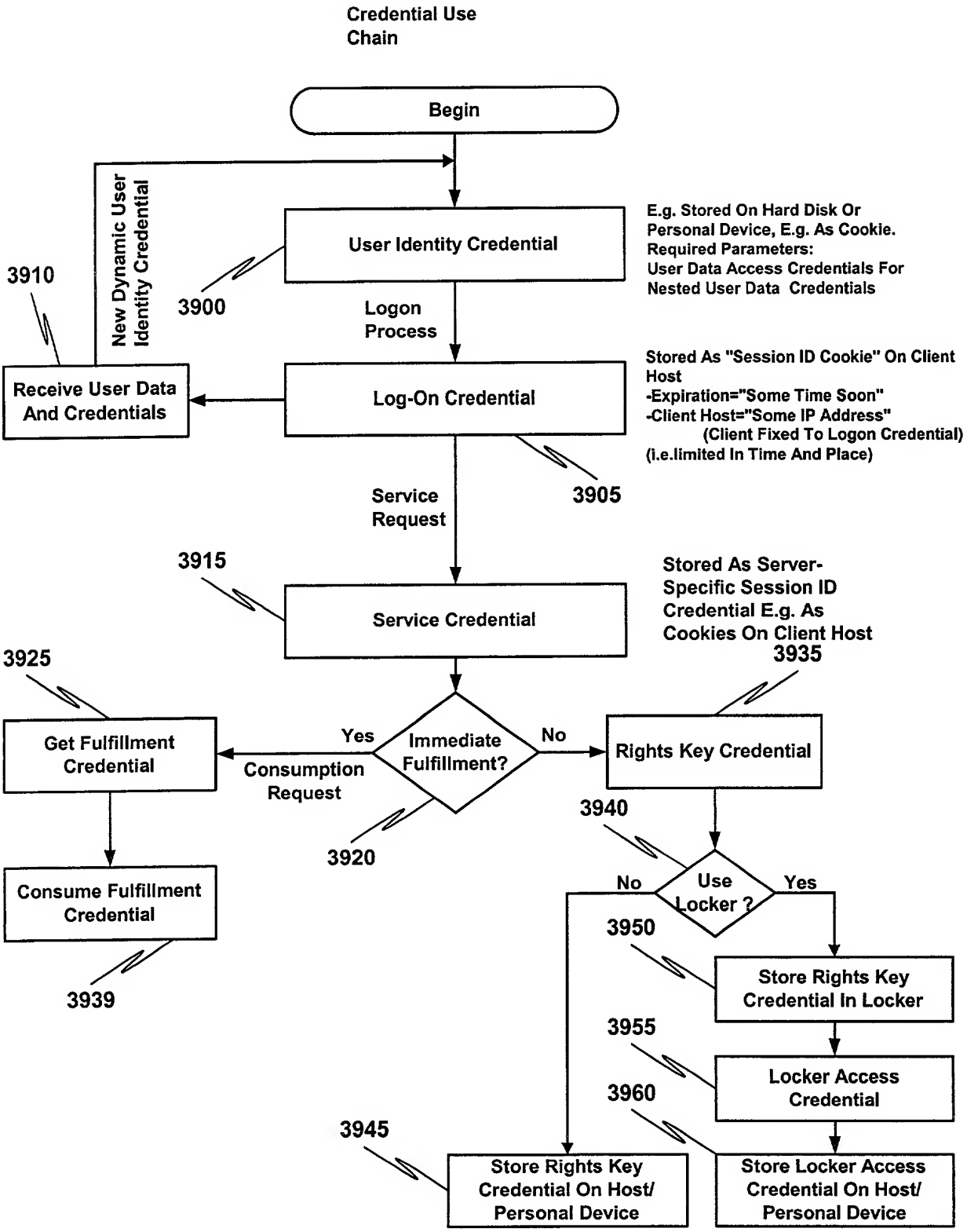
Credential Use Chain
Begin
User Identity Credential
E.g. Stored On Hard Disk Or Personal Device, E.g. As Cookie.
Required Parameters:
User Data Access Credentials For Nested User Data Credentials
3900
3910
New Dynamic User Identity Credential
Logon Process
Receive User Data And Credentials
Log-On Credential
Stored As "Session ID Cookie" On Client Host
-Expiration="Some Time Soon"
-Client Host="Some IP Address"
(Client Fixed To Logon Credential)
(i.e.limited In Time And Place)
3905
Service Request
3915
Service Credential
Stored As Server-Specific Session ID Credential E.g. As Cookies On Client Host
3925
3935
Get Fulfillment Credential
Yes
Immediate Fulfillment?
No
Consumption Request
Rights Key Credential
3920
3940
Consume Fulfillment Credential
No
Use Locker ?
Yes
3939
3950
Store Rights Key Credential In Locker
3955
Locker Access Credential
3960
3945
Store Rights Key Credential On Host/ Personal Device
Store Locker Access Credential On Host/ Personal Device

FIG. 39

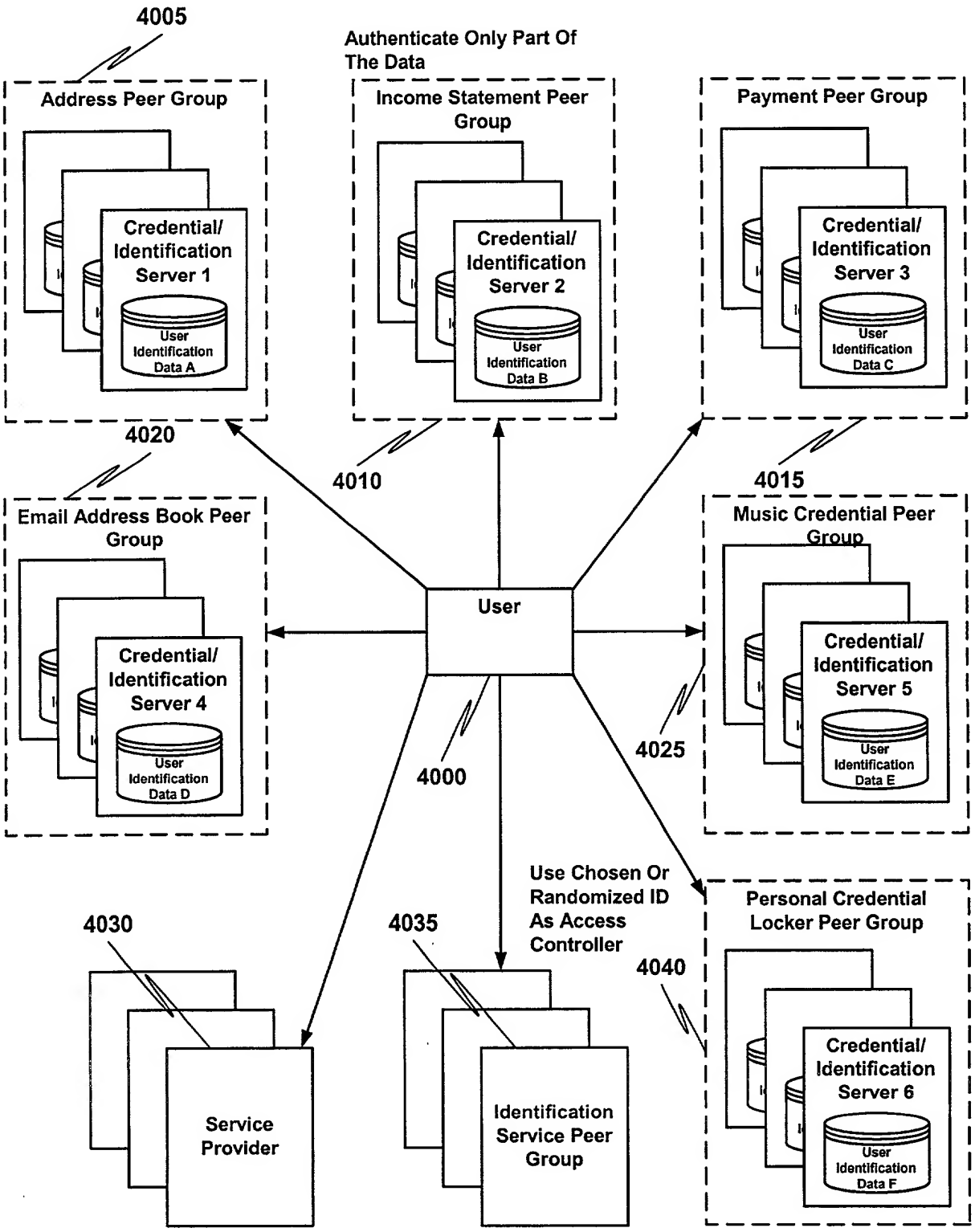
4005
Authenticate Only Part Of The Data
Address Peer Group
Credential/ Identification Server 1
User Identification Data A
Income Statement Peer Group
Credential/ Identification Server 2
User Identification Data B
Payment Peer Group
Credential/ Identification Server 3
User Identification Data C
4020
4010
4015
Email Address Book Peer Group
Credential/ Identification Server 4
User Identification Data D
User
Music Credential Peer Group
Credential/ Identification Server 5
User Identification Data E
4000
4025
Use Chosen Or Randomized ID As Access Controller
4030
4035
4040
Personal Credential Locker Peer Group
Credential/ Identification Server 6
User Identification Data F
Service Provider
Identification Service Peer Group

FIG. 40

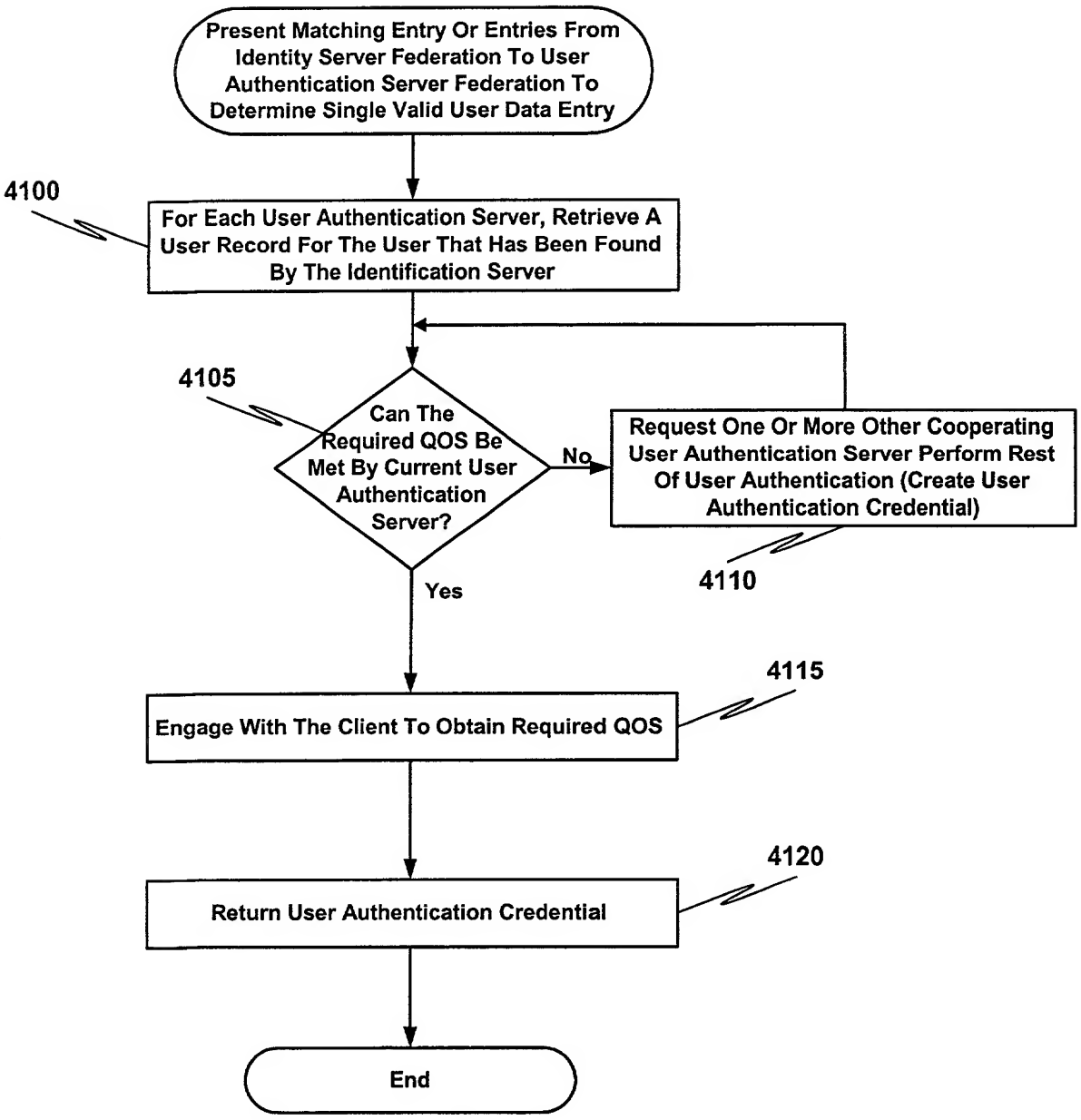
Present Matching Entry Or Entries From Identity Server Federation To User Authentication Server Federation To Determine Single Valid User Data Entry
4100
For Each User Authentication Server, Retrieve A User Record For The User That Has Been Found By The Identification Server
4105
Can The Required QOS Be Met By Current User Authentication Server?
No
Request One Or More Other Cooperating User Authentication Server Perform Rest Of User Authentication (Create User Authentication Credential)
4110
Yes
4115
Engage With The Client To Obtain Required QOS
4120
Return User Authentication Credential
End

FIG. 41

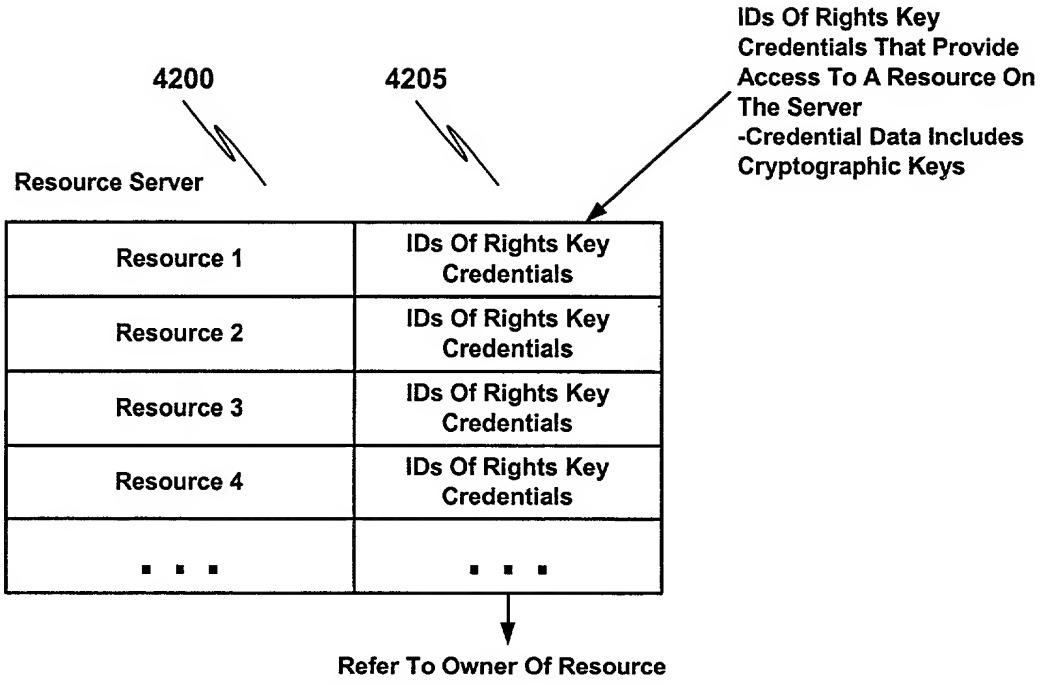


FIG. 42A

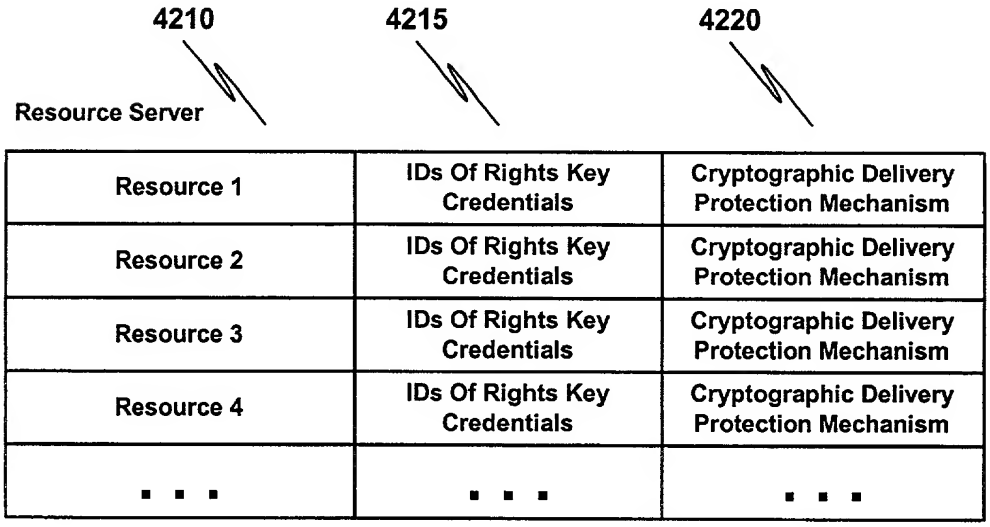


FIG. 42B

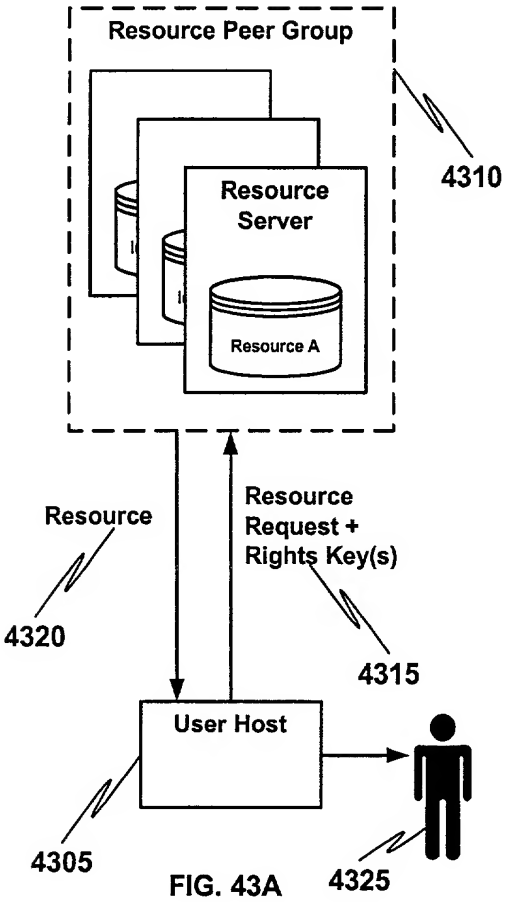


FIG. 43A

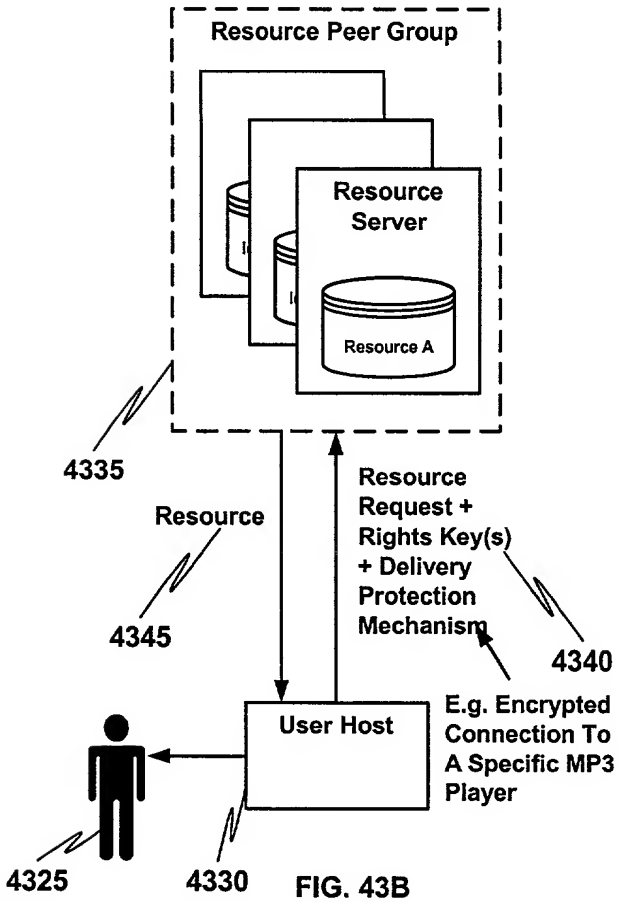


FIG. 43B

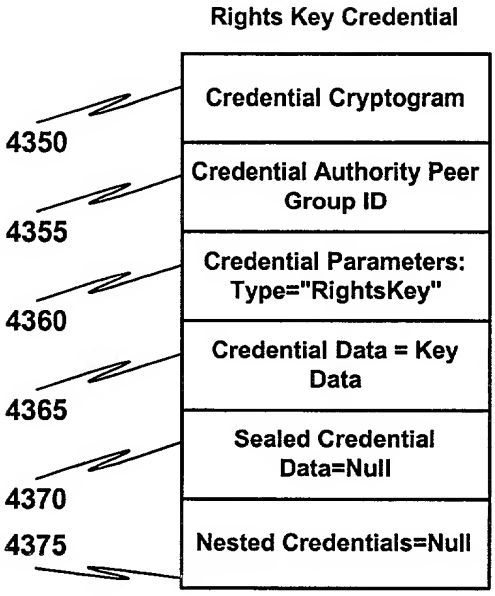


FIG. 43C

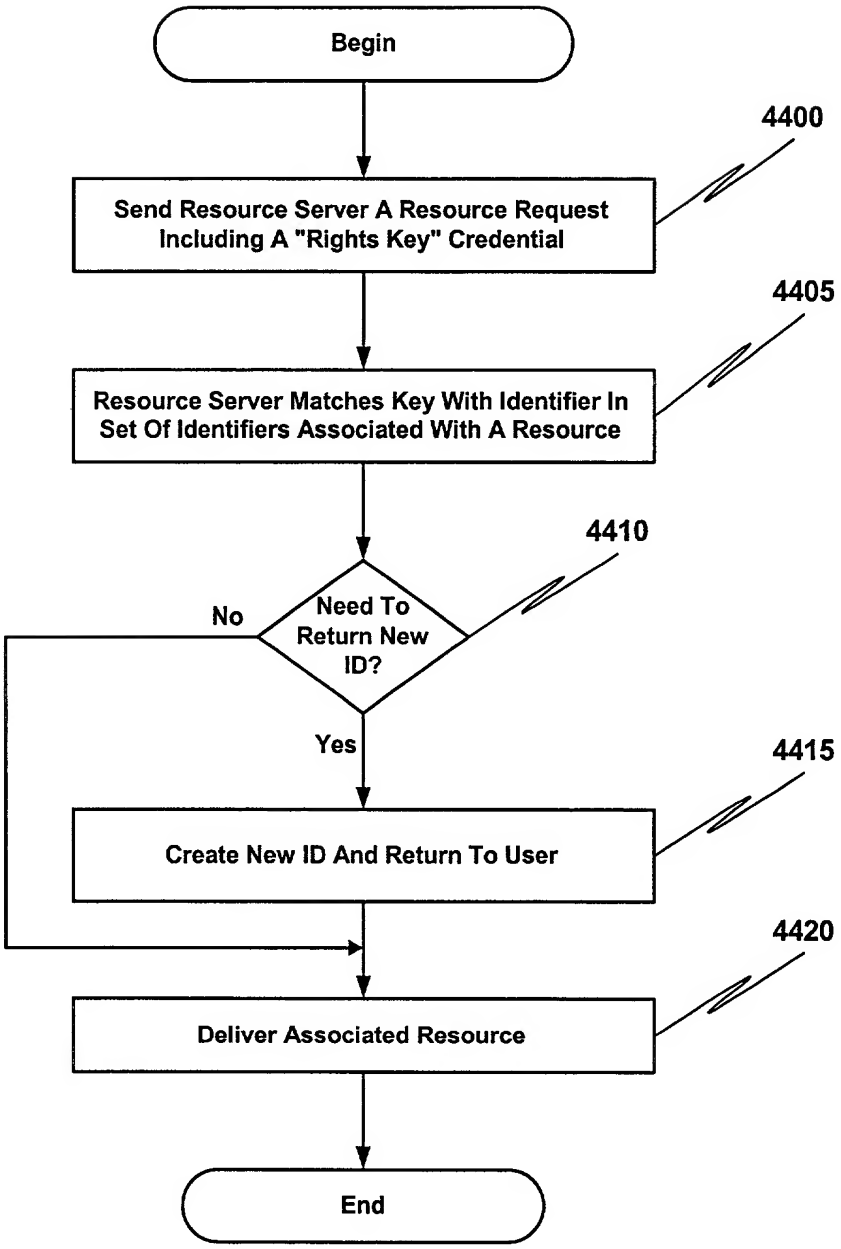
Begin
4400
Send Resource Server A Resource Request Including A "Rights Key" Credential
4405
Resource Server Matches Key With Identifier In Set Of Identifiers Associated With A Resource
4410
Need To Return New ID?
No
Yes
4415
Create New ID And Return To User
4420
Deliver Associated Resource
End

FIG. 44

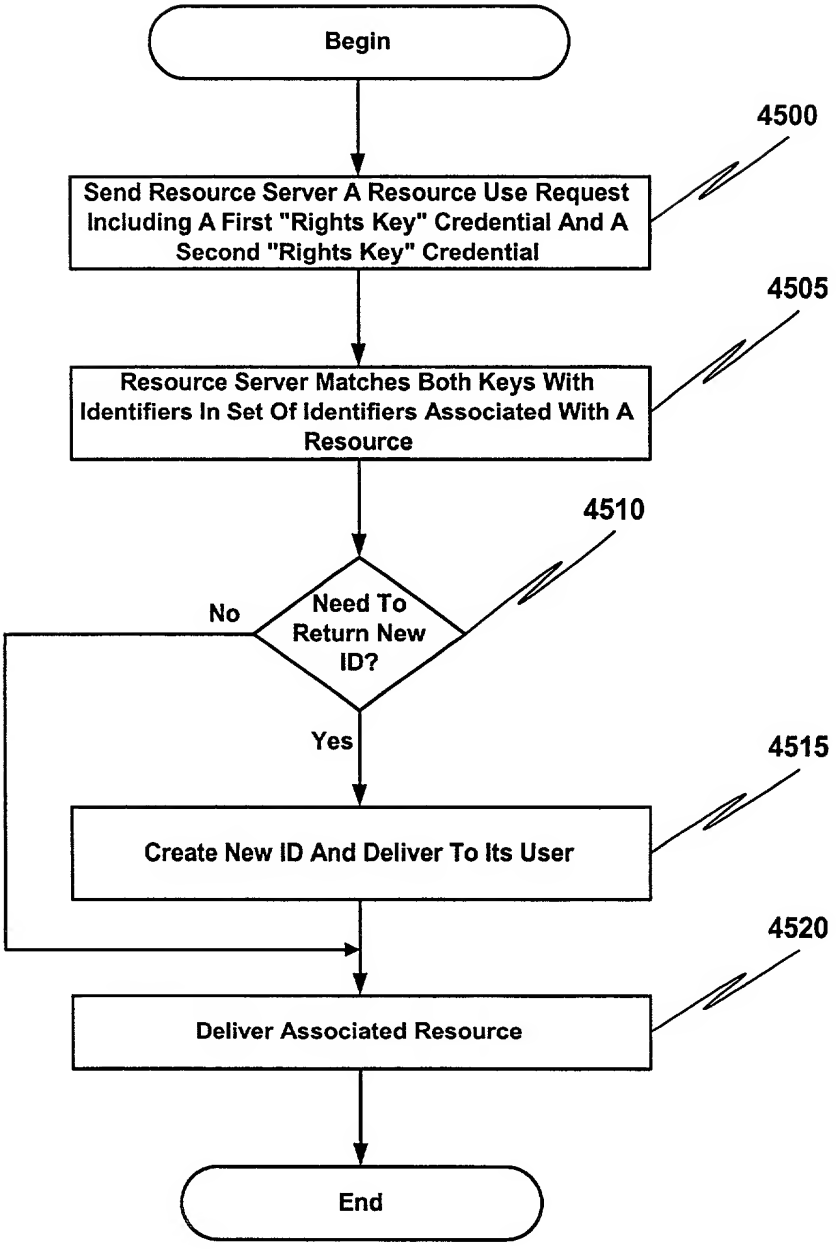
Begin
4500
Send Resource Server A Resource Use Request Including A First "Rights Key" Credential And A Second "Rights Key" Credential
4505
Resource Server Matches Both Keys With Identifiers In Set Of Identifiers Associated With A Resource
4510
Need To Return New ID?
No
Yes
4515
Create New ID And Deliver To Its User
4520
Deliver Associated Resource
End

FIG. 45

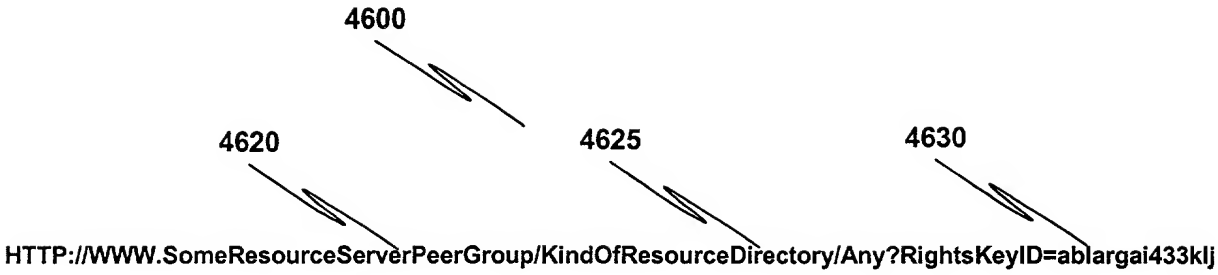


FIG. 46A

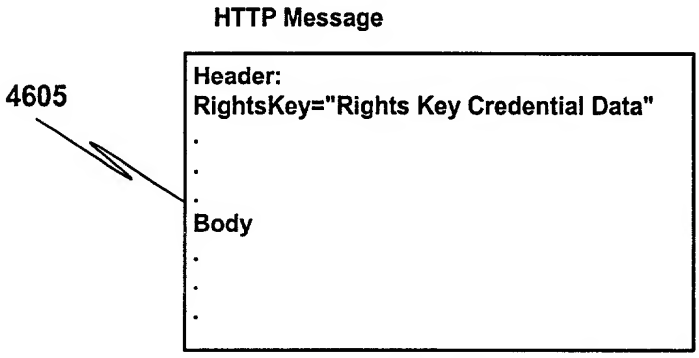


FIG. 46B

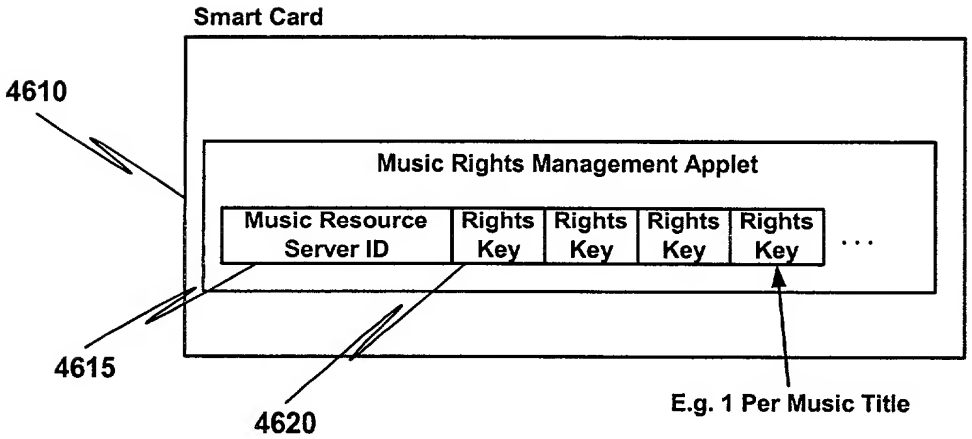


FIG. 46C

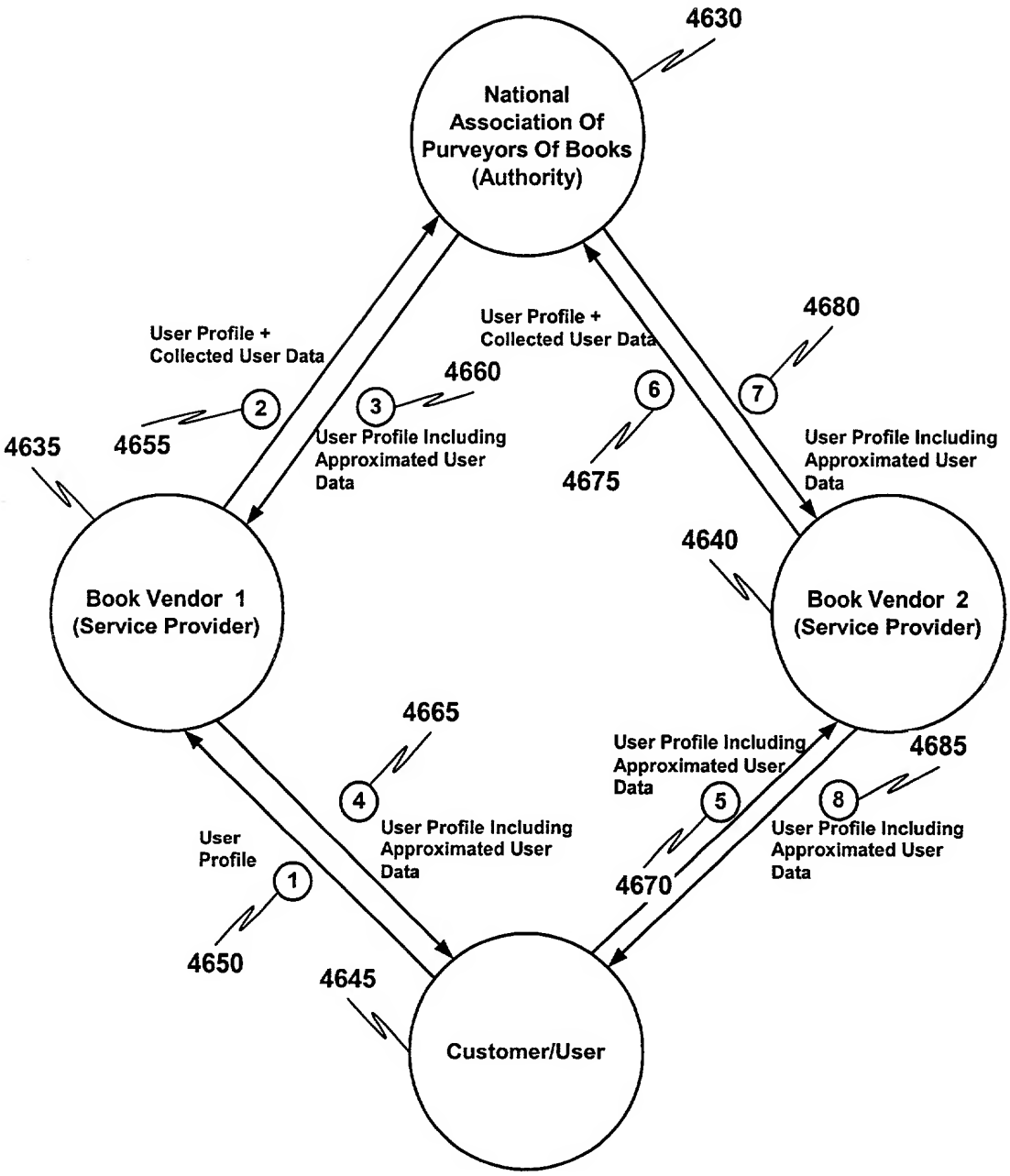
4630
National Association Of Purveyors Of Books (Authority)
User Profile + Collected User Data
2
4655
4635
3
4660
User Profile Including Approximated User Data
User Profile + Collected User Data
6
4675
7
4680
User Profile Including Approximated User Data
Book Vendor 1 (Service Provider)
4640
Book Vendor 2 (Service Provider)
4665
4
User Profile Including Approximated User Data
User Profile Including Approximated User Data
5
4670
4685
8
User Profile Including Approximated User Data
User Profile
1
4650
4645
Customer/User

FIG. 46D

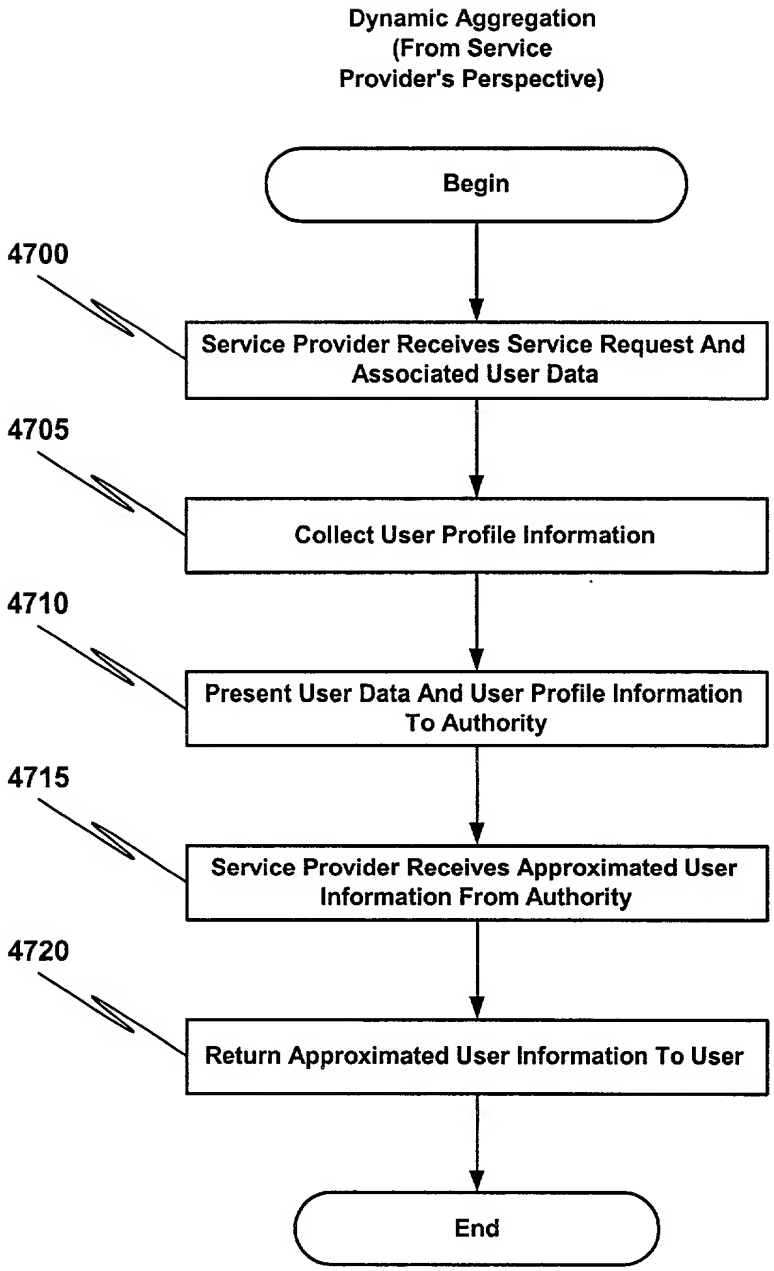
Dynamic Aggregation
(From Service
Provider's Perspective)
Begin
4700
Service Provider Receives Service Request And Associated User Data
4705
Collect User Profile Information
4710
Present User Data And User Profile Information To Authority
4715
Service Provider Receives Approximated User Information From Authority
4720
Return Approximated User Information To User
End

FIG. 47

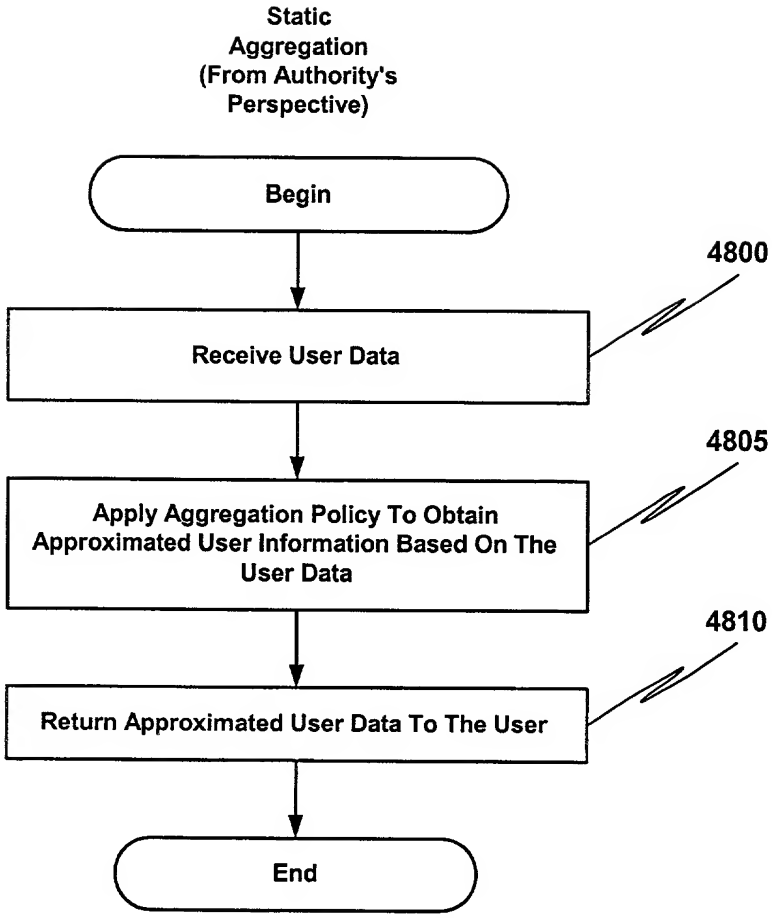
Static
Aggregation
(From Authority's
Perspective)
Begin
4800
Receive User Data
4805
Apply Aggregation Policy To Obtain
Approximated User Information Based On The
User Data
4810
Return Approximated User Data To The User
End

FIG. 48

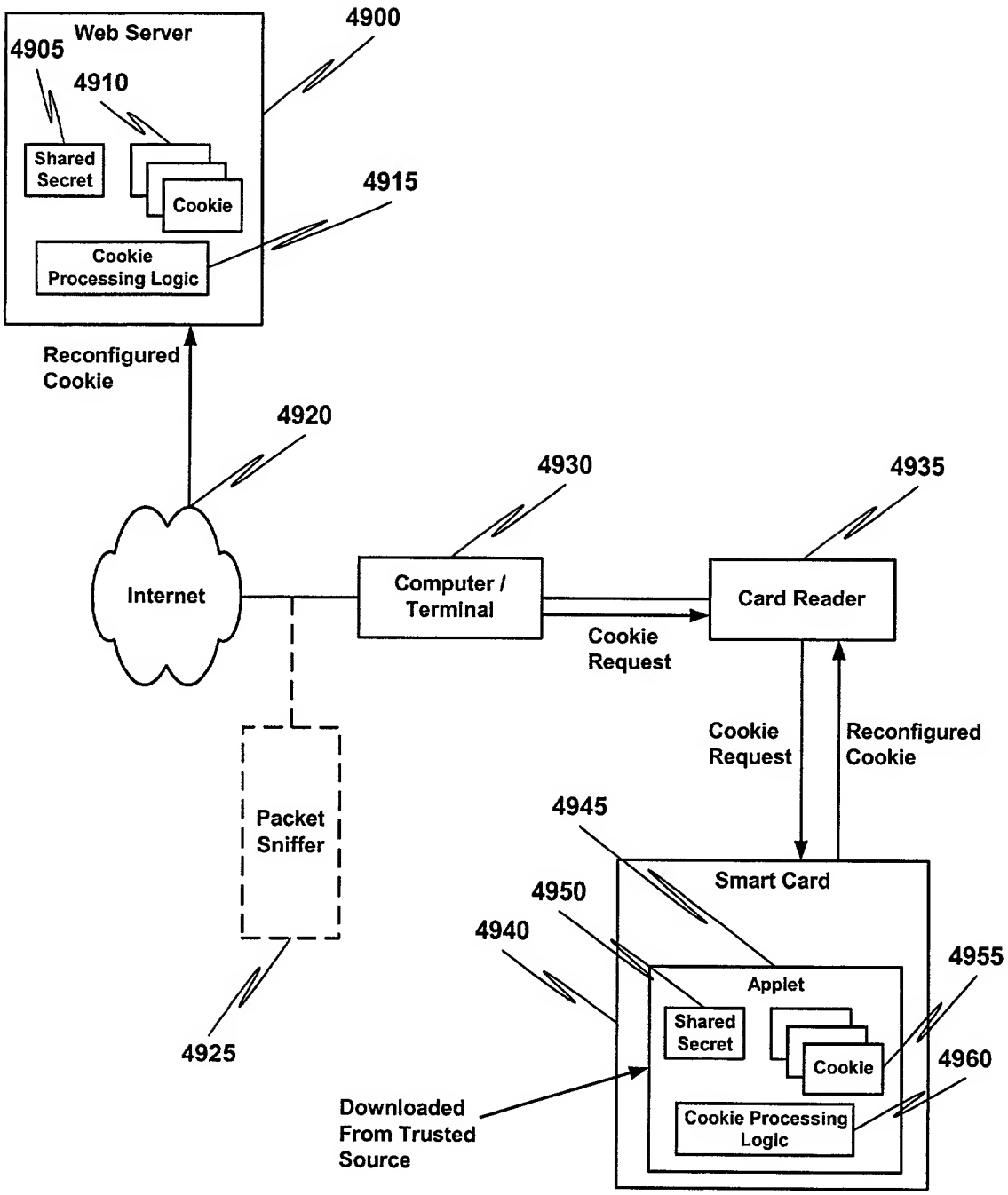
Web Server
4900
4905
4910
Shared Secret
Cookie
4915
Cookie Processing Logic
Reconfigured Cookie
4920
4930
4935
Internet
Computer / Terminal
Card Reader
Cookie Request
Cookie Request
Reconfigured Cookie
Packet Sniffer
4945
Smart Card
4950
4940
4955
Applet
Shared Secret
Cookie
4960
Cookie Processing Logic
Downloaded From Trusted Source
4925

FIG. 49

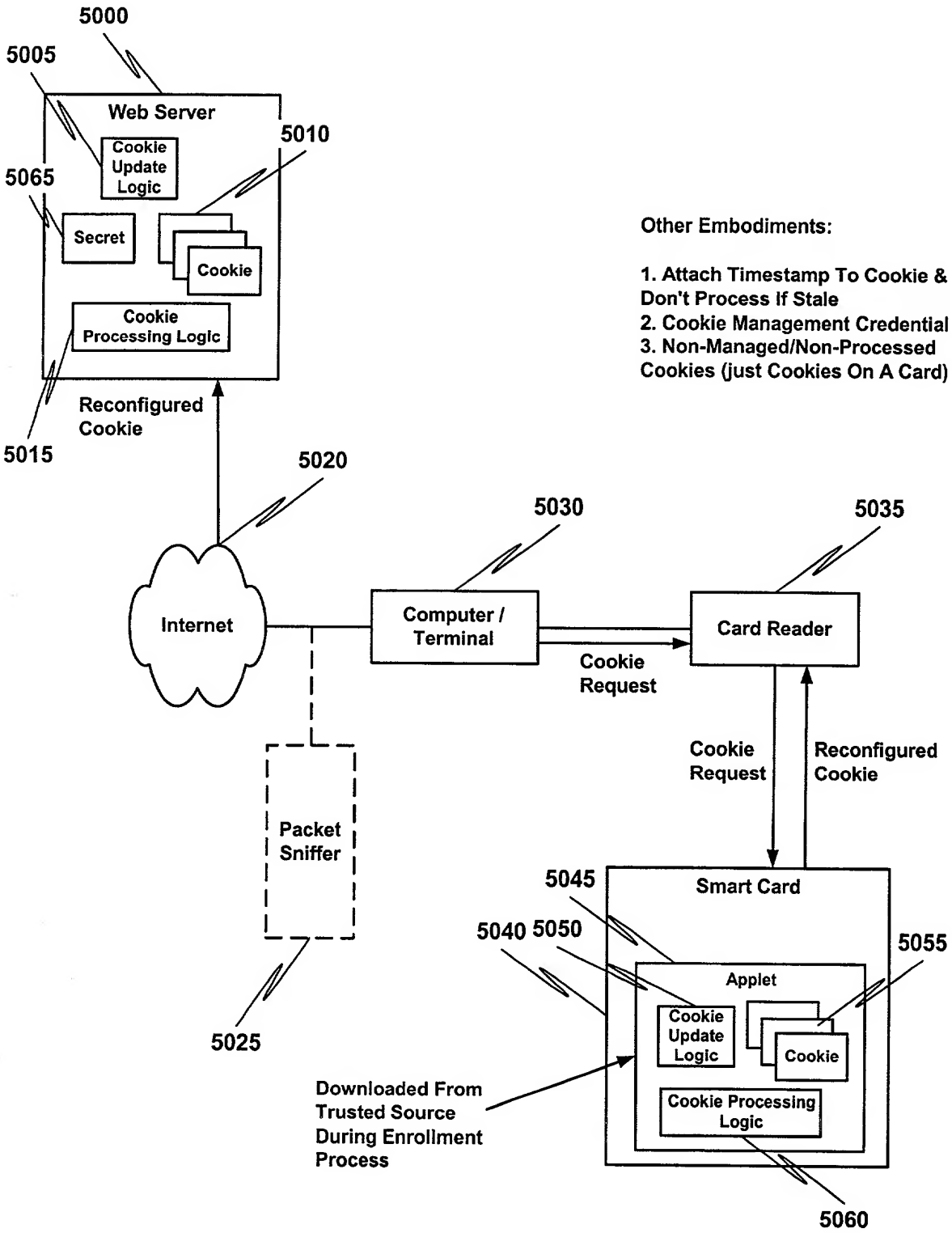
5000
5005
Web Server
Cookie Update Logic
5010
5065
Secret
Cookie
Cookie Processing Logic
Reconfigured Cookie
5015
Other Embodiments:
1. Attach Timestamp To Cookie & Don't Process If Stale
2. Cookie Management Credential
3. Non-Managed/Non-Processed Cookies (just Cookies On A Card)
5020
5030
5035
Internet
Computer / Terminal
Card Reader
Cookie Request
Cookie Request
Reconfigured Cookie
Packet Sniffer
5045
Smart Card
5040 5050
5055
Applet
Cookie Update Logic
Cookie
Cookie Processing Logic
Downloaded From Trusted Source During Enrollment Process
5025
5060

FIG. 50

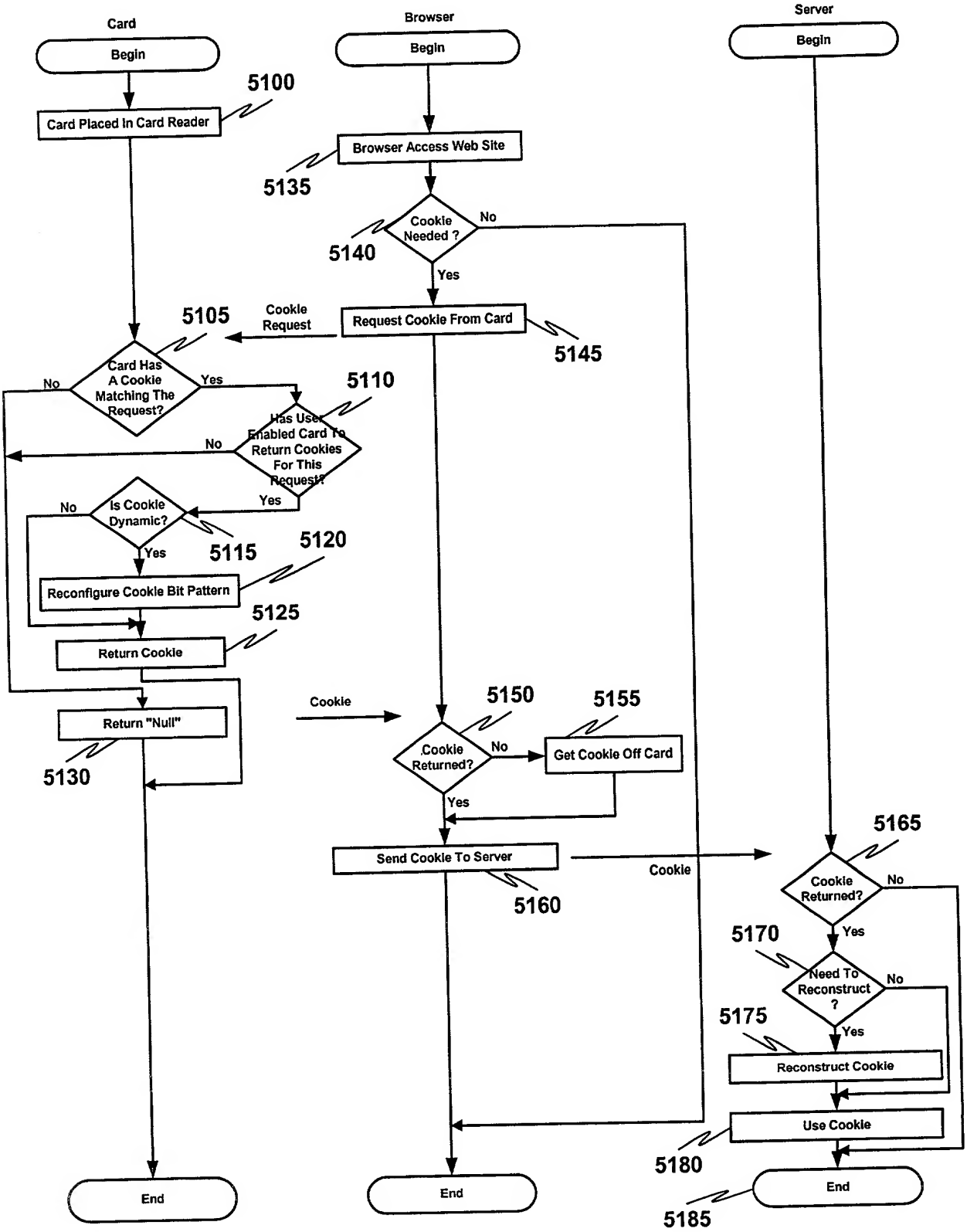
Card
Begin
5100
Card Placed In Card Reader
Browser
Begin
Browser Access Web Site
5135
Cookie Needed ?
5140
No
Yes
Server
Begin
5105
Cookie Request
Request Cookie From Card
5145
Card Has A Cookie Matching The Request?
No
Yes
5110
Has User Enabled Card To Return Cookies For This Request?
No
Yes
Is Cookie Dynamic?
No
Yes
5115
5120
Reconfigure Cookie Bit Pattern
5125
Return Cookie
Return "Null"
5130
End
Cookie
5150
Cookie Returned?
No
5155
Get Cookie Off Card
Yes
Send Cookie To Server
5160
End
Cookie
5165
Cookie Returned?
No
Yes
5170
Need To Reconstruct ?
No
Yes
5175
Reconstruct Cookie
Use Cookie
5180
End
5185

FIG. 51